可下载教学资料

http://www.tup.tsinghua.edu.cn

高等学校教材

信息管理与信息系统

计算机信息安全管理实验教程

魏红芹 编著

清华大学出版社

高等学校教材·信息管理与信息系统

计算机信息安全管理实验教程

魏红芹　编著

清华大学出版社
北　京

内 容 简 介

本实验教材面向计算机和管理交叉类专业学生，从信息安全管理的角度出发，对信息系统整体安全体系进行分析和实验设计。书中针对技术基础和综合安全管理两个方面设计了详细实用的学习和练习手册，体现了“技术与管理”并重的信息安全观念，使得读者可以获得较为全面的专业技能，也便于教师根据课程进行选用。全书共包括5章、27个实验，涵盖了操作系统平台安全、网络安全、计算机病毒防治、应用系统安全、信息系统综合安全管理等领域。对于每个实验书中都给出了详尽的操作步骤说明和图示，容易理解和掌握。另外，还对各实验进行分析总结，便于使用者对实验举一反三，深入思考。

本书适合信息管理与信息系统、电子商务及计算机等专业学生及企业信息系统安全管理人员使用。

本书封面贴有清华大学出版社防伪标签，无标签者不得销售。
版权所有，侵权必究。侵权举报电话：010-62782989　13701121933

图书在版编目(CIP)数据

计算机信息安全管理实验教程/魏红芹编著. —北京：清华大学出版社，2010.4
(高等学校教材·信息管理与信息系统)
ISBN 978-7-302-22201-9

Ⅰ.①计…　Ⅱ.①魏…　Ⅲ.①电子计算机—安全技术—高等学校—教材　Ⅳ.①TP309

中国版本图书馆 CIP 数据核字(2010)第036598号

责任编辑：闫红梅
责任校对：焦丽丽
责任印制：

出版发行：清华大学出版社　　**地　址**：北京清华大学学研大厦A座
http://www.tup.com.cn　　**邮　编**：100084
社 总 机：010-62770175　　**邮　购**：010-62786544
投稿与读者服务：010-62776969，c-service@tup.tsinghua.edu.cn
质 量 反 馈：010-62772015，zhiliang@tup.tsinghua.edu.cn
印 刷 者：
装 订 者：
经　销：全国新华书店
开　本：185×260　　**印　张**：8.75　　**字　数**：212千字
版　次：2010年4月第1版　　**印　次**：2010年4月第1次印刷
印　数：1～　000
定　价：　.00元

产品编号：

出版说明

改革开放以来，特别是党的十五大以来，我国教育事业取得了举世瞩目的辉煌成就，高等教育实现了历史性的跨越，已由精英教育阶段进入国际公认的大众化教育阶段。在质量不断提高的基础上，高等教育规模取得如此快速的发展，创造了世界教育发展史上的奇迹。当前，教育工作既面临着千载难逢的良好机遇，同时也面临着前所未有的严峻挑战。社会不断增长的高等教育需求同教育供给特别是优质教育供给不足的矛盾，是现阶段教育发展面临的基本矛盾。

教育部一直十分重视高等教育质量工作。2001 年 8 月，教育部下发了《关于加强高等学校本科教学工作，提高教学质量的若干意见》，提出了十二条加强本科教学工作提高教学质量的措施和意见。2003 年 6 月和 2004 年 2 月，教育部分别下发了《关于启动高等学校教学质量与教学改革工程精品课程建设工作的通知》和《教育部实施精品课程建设提高高校教学质量和人才培养质量》文件，指出"高等学校教学质量和教学改革工程"是教育部正在制定的《2003—2007 年教育振兴行动计划》的重要组成部分，精品课程建设是"质量工程"的重要内容之一。教育部计划用五年时间(2003—2007 年)建设 1500 门国家级精品课程，利用现代化的教育信息技术手段将精品课程的相关内容上网并免费开放，以实现优质教学资源共享，提高高等学校教学质量和人才培养质量。

为了深入贯彻落实教育部《关于加强高等学校本科教学工作，提高教学质量的若干意见》精神，紧密配合教育部已经启动的"高等学校教学质量与教学改革工程精品课程建设工作"，在有关专家、教授的倡议和有关部门的大力支持下，我们组织并成立了"清华大学出版社教材编审委员会"(以下简称"编委会")，旨在配合教育部制定精品课程教材的出版规划，讨论并实施精品课程教材的编写与出版工作。"编委会"成员皆来自全国各类高等学校教学与科研第一线的骨干教师，其中许多教师为各校相关院、系主管教学的院长或系主任。

按照教育部的要求，"编委会"一致认为，精品课程的建设工作从开始就要坚持高标准、严要求，处于一个比较高的起点上；精品课程教材应该能够反映各高校教学改革与课程建设的需要，要有特色风格、有创新性(新体系、新内容、新手段、新思路，教材的内容体系有较高的科学创新、技术创新和理念创新的含量)、先进性(对原有的学科体系有实质性的改革和发展，顺应并符合新世纪教学发展的规律，代表并引领课程发展的趋势和方向)、示范性(教材所体现的课程体系具有较广泛的辐射性和示范性)和一定的前瞻

性。教材由个人申报或各校推荐(通过所在高校的“编委会”成员推荐),经“编委会”认真评审,最后由清华大学出版社审定出版。

目前,针对计算机类和电子信息类相关专业成立了两个“编委会”,即“清华大学出版社计算机教材编审委员会”和“清华大学出版社电子信息教材编审委员会”。首批推出的特色精品教材包括:

(1)高等学校教材·计算机应用——高等学校各类专业,特别是非计算机专业的计算机应用类教材。

(2)高等学校教材·计算机科学与技术——高等学校计算机相关专业的教材。

(3)高等学校教材·电子信息——高等学校电子信息相关专业的教材。

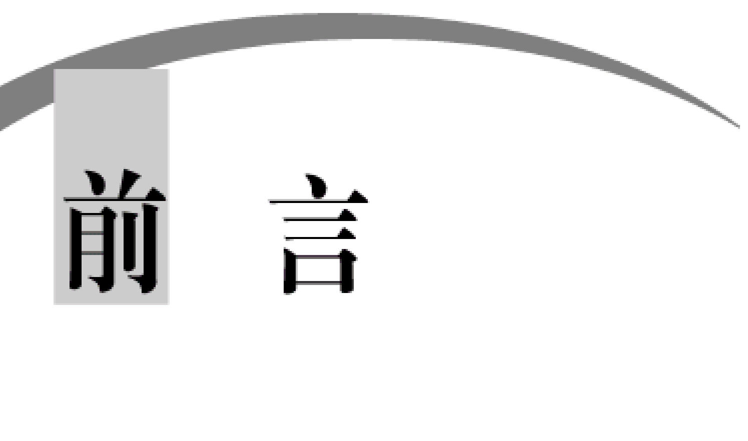
(4)高等学校教材·软件工程——高等学校软件工程相关专业的教材。

(5)高等学校教材·信息管理与信息系统。

(6)高等学校教材·财经管理与计算机应用。

清华大学出版社经过20多年的努力,在教材尤其是计算机和电子信息类专业教材出版方面树立了权威品牌,为我国的高等教育事业做出了重要贡献。清华版教材形成了技术准确、内容严谨的独特风格,这种风格将延续并反映在特色精品教材的建设中。

清华大学出版社教材编审委员会
E-mail:dingl@tup.tsinghua.edu.cn



计算机安全问题是伴随着计算机的发展而产生的。随着互联网的日益普及和各种信息技术在各行业得到越来越广泛的应用，整个社会对信息系统的依赖程度日益提高，安全问题也变得越来越复杂和重要。面对各种严重的计算机信息系统安全威胁，关于信息安全的研究开始得到人们的重视。目前，信息安全已经成为信息科学领域重要的研究课题，众多高等院校也相应开设了信息安全专业和课程。

在计算机信息安全的教学中，学生的实践活动是非常重要的一个环节，通过实际动手参与操作实验，学生可以更好地理解相关理论知识，增加感性认识，提高解决实际问题的能力。如何根据教学目标，针对学生的知识结构，设计出恰当的实验项目也是信息安全教学中需要解决的问题。信息安全作为一门综合性学科，课程内容覆盖面广，不同学院和专业开设的安全课程往往有不同的侧重点，对于信息系统和信息管理专业的学生来讲，在课程设计上管理和计算机技术兼重，相对而言一些底层的技术细节略有弱化，但是对于全局的把握和管理方面则要求较高。

本书从信息安全管理的角度出发，对信息系统整体安全体系进行分析和构建，突破该领域存在的“重技术，轻管理”的传统思想，有助于获得系统全面和真正的安全。书中从操作系统平台安全、网络安全、计算机病毒防治、应用系统安全、信息系统综合安全管理等方面设计了5章、27个实验。对于每个实验，在对信息安全工作人员需要具备的基本知识和技能进行总结的基础上，给出了实际的操作方案和训练途径，使读者易于理解和掌握实验的原理和实验操作方法。同时也充分考虑了实验开设的便利性，大部分实验都可以在普通的计算机和系统平台上完成，实验软件也主要选用一些易获得的免费版本。本教材中各实验相对独立，可以用于独立性信息安全实验课程，也可供相关课程在开设课内实验时进行部分选用。

本书中内容已被多次应用在东华大学管理学院信息系统和信息管理专业的计算机信息安全实验教学中，并且取得了较好的效果。本书在编写过程中，得到了东华大学管理学院姚卫新、曹海生、陈梅梅等老师的热情帮助，也得到了东华大学管理学院经济贸易实验室各位老师的大力帮助，在此表示衷心的感谢。

计算机信息安全课程在各大高校的开设时间相对较短，对于课程的教学方法和教学内容，特别是实践环节的开设方法还在不断探索之中。由于本人能力和水平所限，加上时间仓促，书中难免有错误和疏漏的地方，敬请读者批评指正。

作　者

2010 年 1 月

目 录

第1章

操作系统平台安全

1.1 实验基础

1.1.1 操作系统安全基础

操作系统作为硬件和软件应用之间接口的程序模块、计算机资源的管理者，是保证计算机系统安全的重要基础。操作系统的安全功能主要包括用户认证、存储器保护、文件与I/O设备的访问控制、对一般目标的定位与访问以及控制共享的实现、内部过程的通信与同步等。

操作系统的安全漏洞是威胁系统安全的主要原因，常见的操作系统漏洞有以下几种。

(1) I/O非法访问：操作系统(Operating System，OS)仅在I/O操作初始阶段进行访问检查，使用公共的系统缓冲区。

(2) 访问控制的混乱：安全访问与资源共享间关系处理不善，操作界限不清。

(3) 不完全的中介：完全的中介必须检查每次访问请求以进行适当的审批，不完全的中介则省略必要安全保护造成保护机制不全面。

(4) 操作系统陷门：指为后续使用和发展而预留的管理程序功能，通常对这些功能缺乏严密监控，有可能被用于安全控制。

操作系统安全的核心在于访问控制，即确保主体对客体的访问只能是授权的，且授权策略是安全的，未经授权的访问是不能进行的。进行访问控制的粒度可以是位级、字节级、字级、字段级、文件级、目录级、卷级等。受控目标级别越大，实现访问控制越容易，控制的灵活度则随之降低。

1.1.2 Windows操作系统安全技术

Windows操作系统在PC上的垄断地位，使其成为应用最为普遍的操作系统。Windows NT 4.0是系列版本中最早实现C2安全级别的操作系统，其后在对Windows NT进一步完善的基础上Microsoft公司又推出了Windows 2000等操作系统。

Windows 2000提供的安全机制包括以下几方面。

(1) 登录安全：使用三键登录界面，可以防止后台恶意程序运行，并通过输入ID和口

令实现登录，由安全帐号管理器接收 ID 和口令，安全帐号数据库验证 ID 和口令访问令牌（包括用户安全标记、用户名、用户所属组等信息）。

（2）设置登录安全：管理员可以使用域用户管理器为用户建立和修改用户属性、安全属性，并设置工作站登录限制、时间登录限制、帐号失效日期、用户登录失败次数等。

（3）文件与目录存取控制：有系统审计、允许访问、禁止访问等几种方式。禁止总是比允许的优先级高，没有设定存取控制的列表的对象采用系统默认值，并自动继承其所处目录的存取控制属性。

（4）用户权限：包括从网络上访问某台计算机、使用特定资源、进行特定操作的权限等。

（5）所有权：文件或目录有自己的拥有者，通常是其创建者。用户不能放弃自己对某对象的所有权，使拥有者对自己创建的对象负责。

（6）访问许可权：提供对文件或目录的读、写、修改、添加、列示、完全控制等访问方式。

（7）共享许可权：对网络共享资源的访问控制。

（8）审计：对可能危及系统安全的系统级属性进行逻辑评估，跟踪并报道企图对系统进行破坏的行为（与监视器和入侵检测器结合）。

（9）备份：制作系统紧急启动盘，备份系统及应用的配置数据，备份用户数据，系统工具，用户备份，第三方备份工具（磁盘备份工具等）。

Windows 默认安装通常需要进行安全化，安全化操作系统的过程称为加固，目的是减少漏洞的数量并保护计算机不受威胁或攻击。加固过程的大致步骤为：应用最新的补丁程序，禁用不必要的服务，删除不必要的用户帐户并重命名 Admin 帐户，确保使用复杂的密码，对文件和访问注册表限制许可，启用关键事件的日志，删除不必要的程序。

1.2 实验项目

1.2.1 帐户安全

1. 实验目的

了解 Windows 2000/XP 系统提供的帐户安全机制，掌握相关的安全设置方法，以提高操作系统安全强度。

2. 实验原理

帐户和口令是登录系统的基础，也是众多黑客程序攻击和窃取的对象，因此，系统的帐户和口令的安全是非常重要的。而 Windows 系统的默认设置存在一定的不安全性，这些不安全性常常被攻击者利用，通过各种手段获得合法的帐户，进一步破解口令入侵系统。通过对系统的合理设置可以避免这种安全风险。

3. 实验环境

一台安装 Windows 2000/XP 操作系统的计算机，磁盘格式设置为 NTFS。

4. 实验内容

（1）检查和删除不再使用的帐户，禁用 Guest 帐户；

（2）启用帐户策略；

（3）开机时设置为“不自动显示上次登录帐户”；

（4）禁止枚举帐户名（本地策略\安全选项，选择“对匿名连接的额外限制”，在“本地策略设置”中选择“不允许枚举 SAM 帐户和共享”）。

5. 实验步骤

（1）以管理员身份进入 Windows 2000 Server 系统，启动“程序”|“管理工具”|“计算机管理”|“系统工具”|“本地用户和组”，禁用 Guest 帐户，重命名 Administrator 帐户，对其他用户和组进行属性设置，如图 1.1 所示。

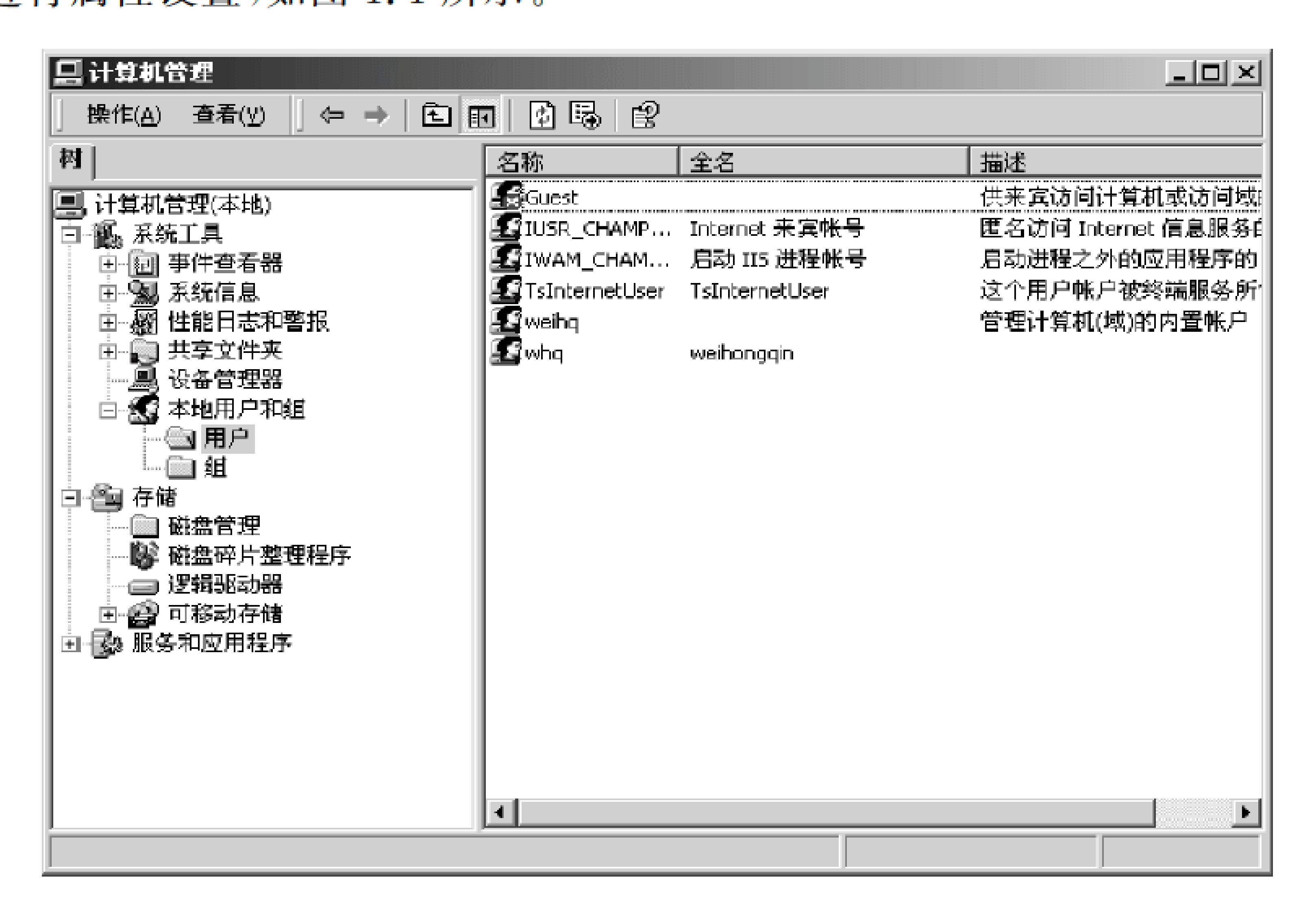


图 1.1　对计算机用户和组属性进行设置

（2）以管理员身份进入 Windows 2000 Server 系统，启动“程序”|“管理工具”|“本地安全策略”|“帐户策略”|“密码策略”，对各项属性分别进行重新设置，如图 1.2 和图 1.3 所示。

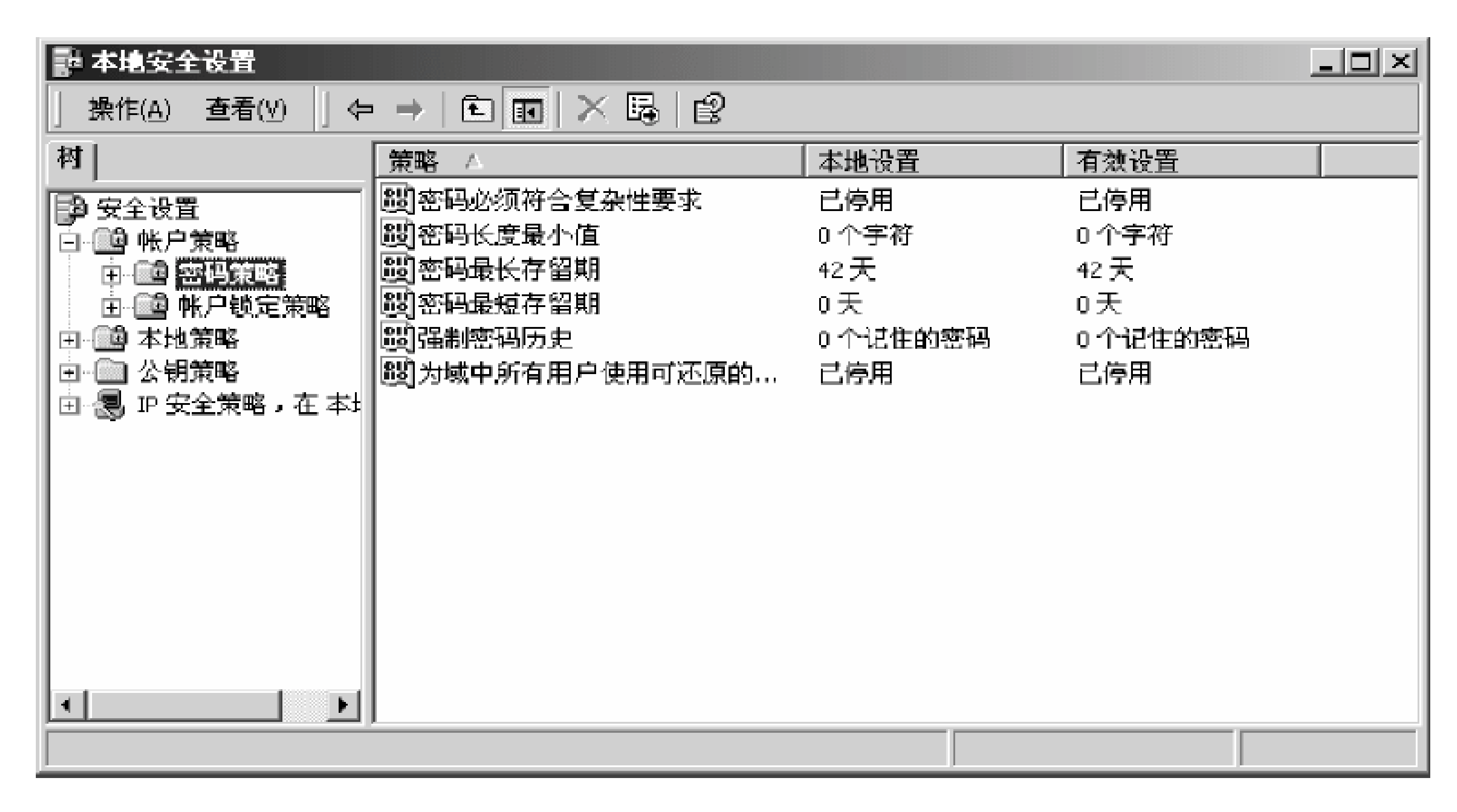


图 1.2　对帐户密码策略进行设置

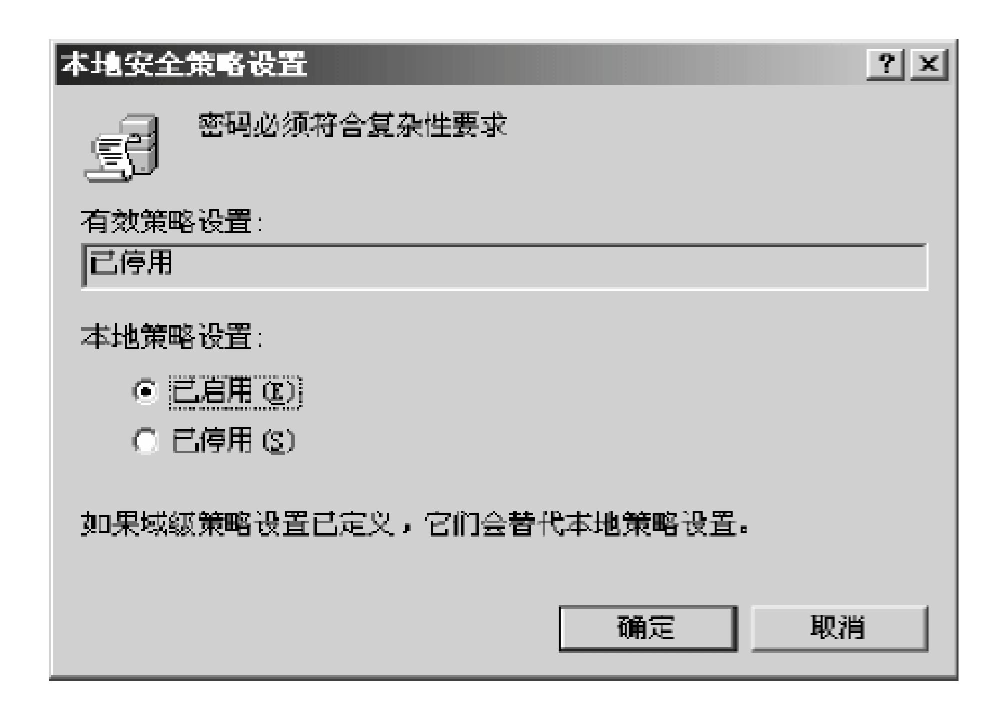


图 1.3 对帐户密码复杂性策略进行设置

(3) 在“帐户锁定策略”中,对各项属性分别进行重新设置,如图 1.4 所示。

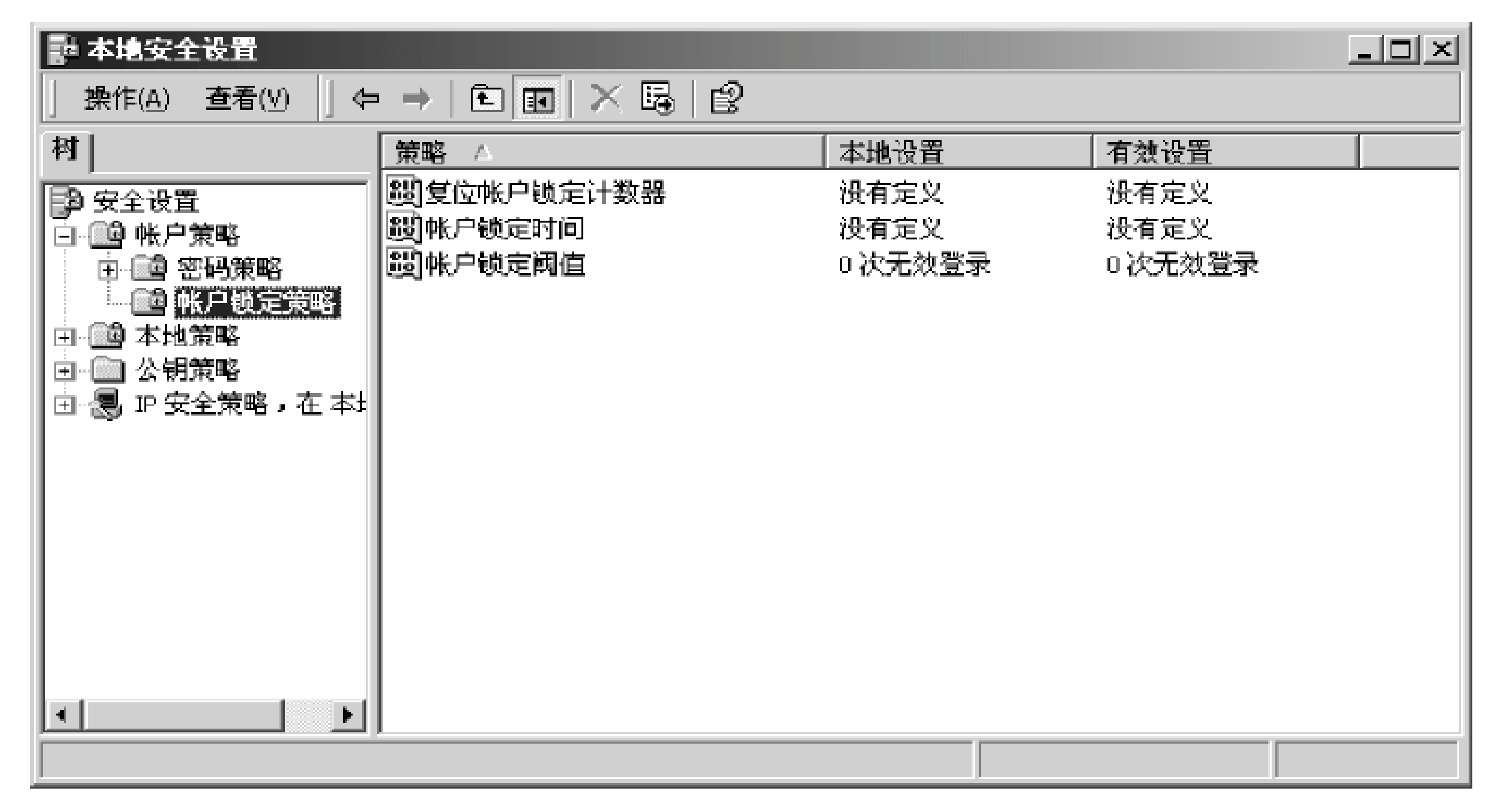


图 1.4 对帐户锁定策略进行设置

(4) 在“本地策略”|“用户权利指派”中,重新设置各权限的所属用户,如图 1.5 和图 1.6 所示。



图 1.5 对用户权限进行设置



图 1.6　对用户权限策略进行设置

(5) 在“本地策略”|“安全选项”中，重新设置各安全选项，如图 1.7 所示。

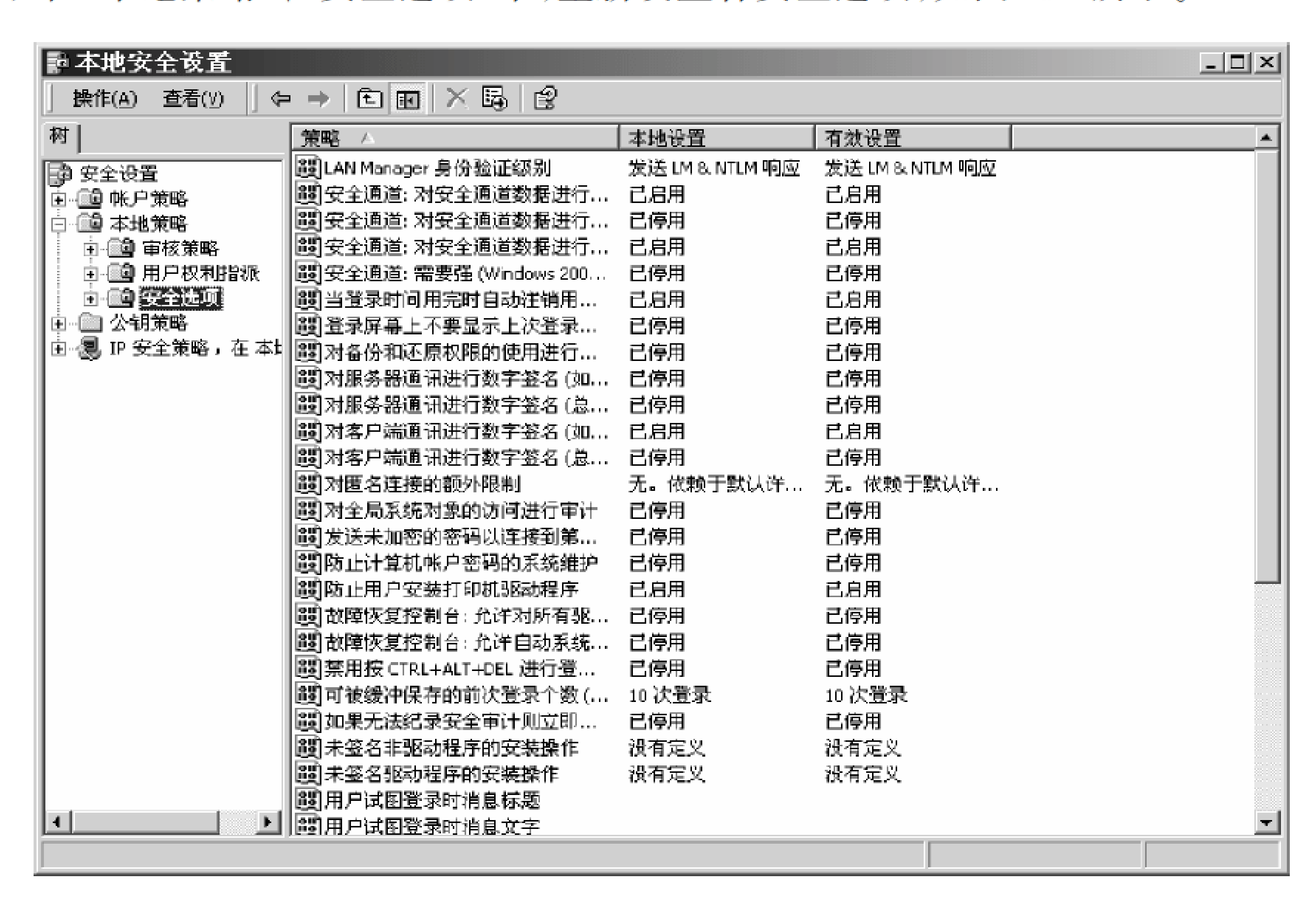


图 1.7　对帐户密码策略进行设置

6. 实验报告与要求

根据上面介绍的各项安全性实验要求，详细观察记录设置前后系统的变化，给出分析报告。

7. 实验分析与讨论

Windows 系统中提供了多种可控的安全选项，对于各选项应该如何设置最为合理，读者可以作进一步思考。

8. 注意事项

(1) Windows 2000 与 Windows XP 操作系统相关设置会稍有不同,但大同小异,以上步骤说明中采用的是 Windows 2000 Server 系统。

(2) 读者可以自行查看"安全选项"中的多项增强系统安全的条目。

1.2.2 日志与审核

1. 实验目的

配置计算机系统以记录安全事件,查看并分析系统事件。

2. 实验原理

日志是所发生事件的清单,每一个日志条目都有事件的日期和时间、事件的类别,以及在哪里可以找到有关该事件的更多信息。计算机安全事故是在系统上发生的任何非法或未经授权的活动。不管计算机是否发生了事故,日志条目都可以显露信息。维护日志很重要,但日志的价值来自于对它们进行的定期检查。Windows 系统中默认地没有进行安全审核,因此需要重新配置想要记录的事件。

3. 实验环境

一台安装 Windows 2000/XP 操作系统的计算机,磁盘格式设置为 NTFS。

4. 实验内容

(1) 在服务器上配置日志审核功能,设置安全性日志和系统日志的保存时间为 14 天。

(2) 设定审核策略如表 1.1 所示。

表 1.1 日志审核策略表

属性	成功	失败
帐号登录	On	On
帐号管理	On	On
目录访问服务	Off	On
登录	On	On
对象访问	Off	On
策略改变	On	On
特权使用	Off	On
进程跟踪	Off	Off
系统	On	On

(3) 执行一定的任务并对日志条目进行分析。

5. 实验步骤

(1) 在"管理工具"|"事件查看器"中,通过右击打开"属性"对话框进行设置,如图 1.8 和图 1.9 所示。



图 1.8　设置"事件查看器"属性



图 1.9　对"安全日志属性"进行设置

(2) 启动"程序"|"管理工具"|"本地安全策略"|"本地策略"|"审核策略",对各审核项目开启情况分别进行重新设置,如图 1.10 和图 1.11 所示。

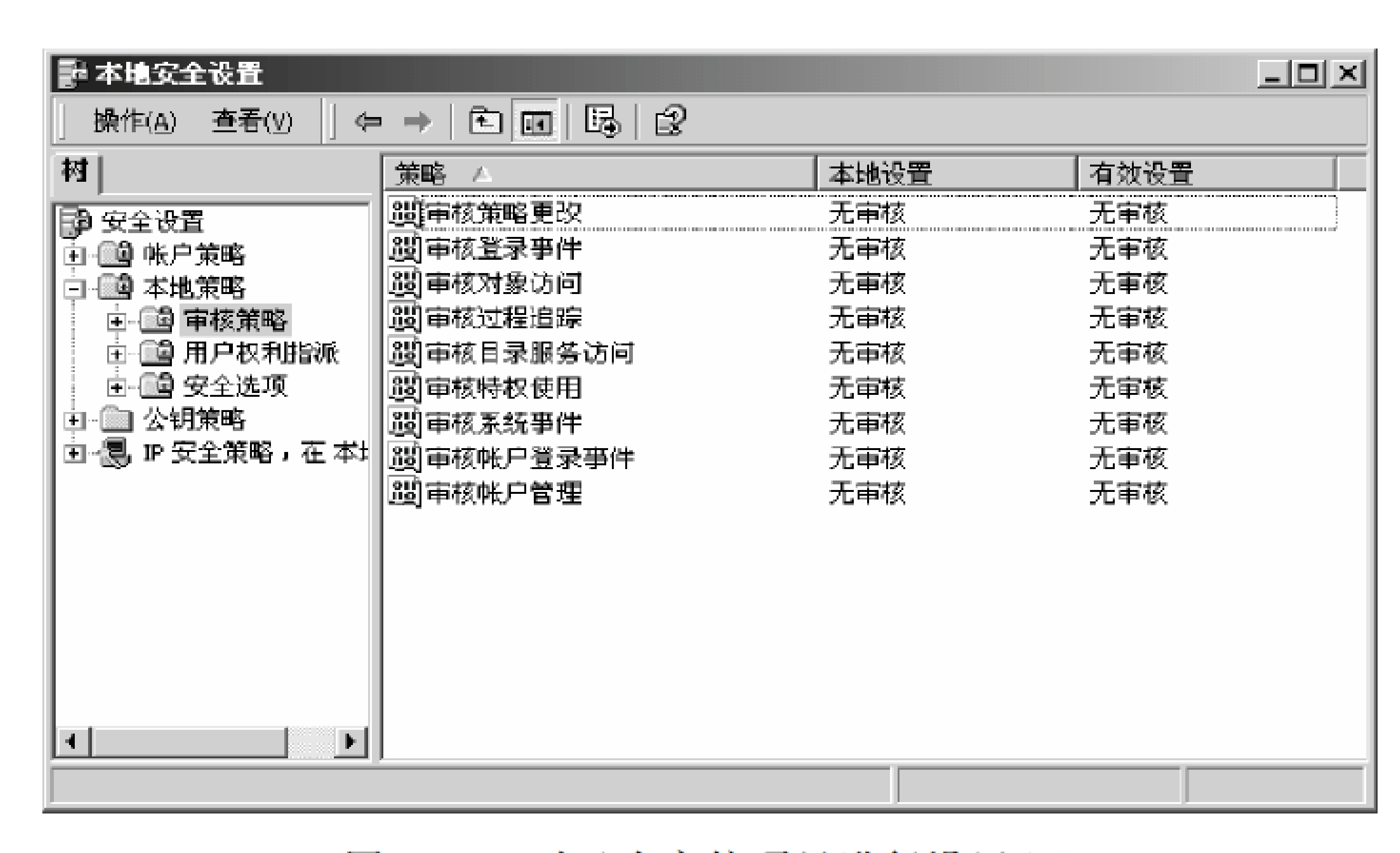


图 1.10　对日志审核项目进行设置(1)



图 1.11　对日志审核项目进行设置(2)

(3) 尝试登录一个不存在的帐户。

(4) 使用一个错误的密码。

(5) 以正式用户的身份登录进去。

(6) 检查系统安全日志,如图 1.12 所示。

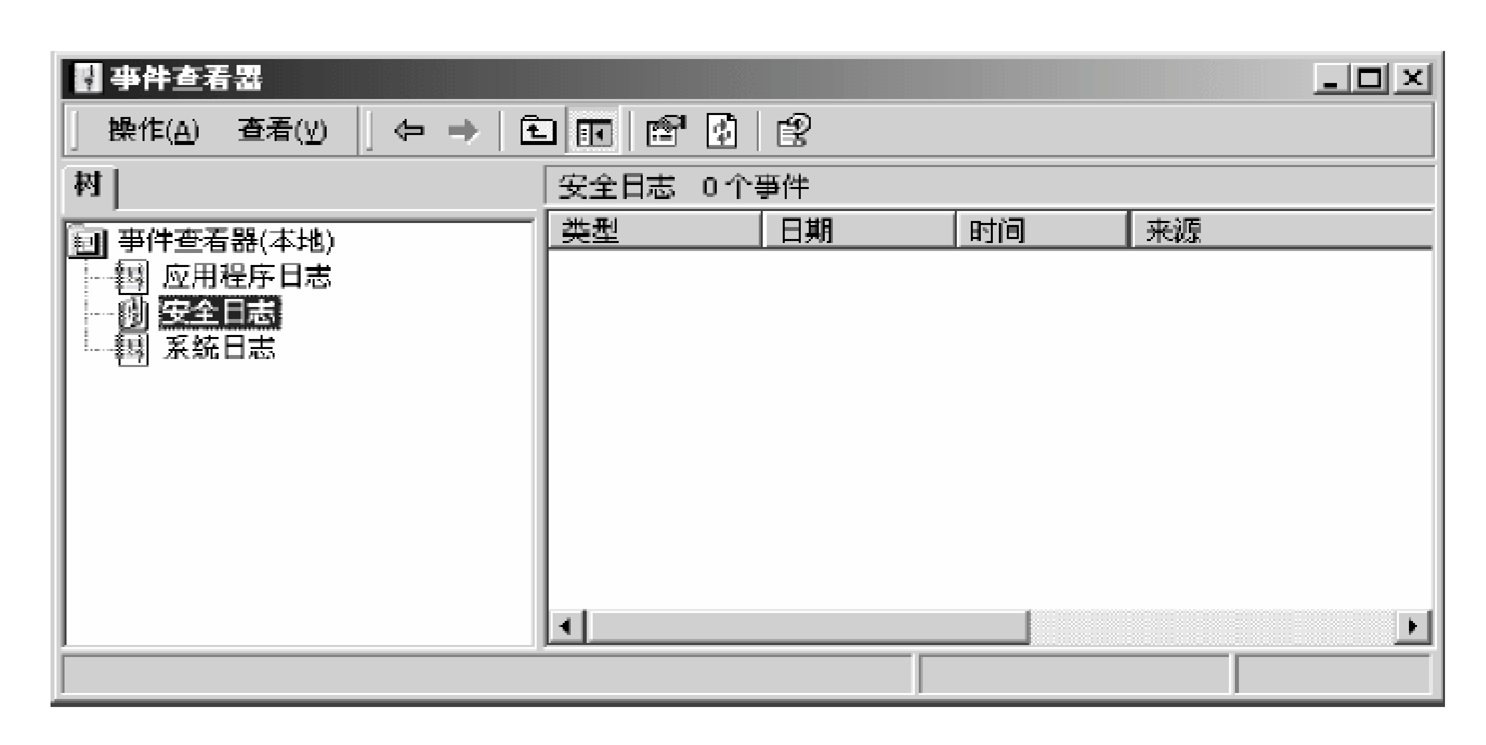


图 1.12　检查系统安全日志

6. 实验报告与要求

根据上面介绍的各项安全性实验要求,详细观察记录设置前后系统的变化,给出分析报告。

7. 实验分析与讨论

安全日志可以记录系统发生的安全事件,但同时条目过多会给管理人员带来过多的工作负担,因此如何取舍需要审核的项目是一个值得考虑和分析的问题。

8. 注意事项

系统日志包括应用程序日志、安全日志和系统日志三部分,分别记录不同类型的系统事

件。进行系统安全管理时，以安全日志内容为主，可以同时结合另外两类事件进行系统分析。

1.2.3 文件资源安全

1. 实验目的

了解 Windows 系统提供的文件资源安全管理功能，掌握其配置方法。

2. 实验原理

磁盘数据被攻击或本地的其他用户破坏和窃取磁盘数据是经常困扰用户的问题。Windows 系统提供的磁盘格式有 FAT、FAT32 以及 NTFS。其中 FAT 和 FAT32 格式没有考虑对安全性方面的更高需求，如无法设置用户访问权限等。NTFS 文件系统是 Windows 操作系统中一种安全的文件系统，管理员或用户可以设置每个文件夹的访问权限，从而限制一些用户和用户组的访问。

NTFS 文件系统还提供了 EFS 功能。EFS 采用了对称和非对称两种加密算法对文件进行加密，首先系统利用生成的对称密钥将文件加密成密文，然后采用 EFS 证书中包含的公钥将对称密钥加密后与密文附加在一起。文件采用 EFS 加密后，可以控制特定的用户有权解密数据，这样即使攻击者能够访问计算机的数据存储器，也无法获取用户数据。只有拥有 EFS 证书的用户，采用证书中公钥对应的私钥，先解密公钥加密的对称密钥，然后再用对称密钥解密密文，才能对文件进行读写操作。

3. 实验环境

采用 NTFS 格式的磁盘，用户具有在 NTFS 卷中修改文件的权限。

4. 实验内容

(1) 新建文件夹 SecurityTest1，常规属性设为只读，共享属性设为所有用户只能读取无法修改；

(2) 新建文件夹 SecurityTest2，设置访问权限为：

- Administrator：完全控制；
- Creator owner：修改、读、写；
- System：完全控制；
- Users：读取、执行、浏览目录；

(3) 对文件夹 SecurityTest1 进行 EFS 加密，并进行验证。

5. 实验步骤

(1) 选中文件夹，通过右击打开属性页进行设置，如图 1.13～图 1.15 所示。

(2) 选中文件夹，通过右击打开“属性”|“安全”选项卡进行设置，如图 1.16 所示。

(3) 选中文件夹，通过右击打开“属性”|“常规”|“高级属性”对话框进行设置，如图 1.17 所示。



图 1.13 对文件夹基本属性进行设置



图 1.14 对文件夹共享属性进行设置



图 1.15 对文件夹权限进行设置



图 1.16 对文件夹安全属性进行设置

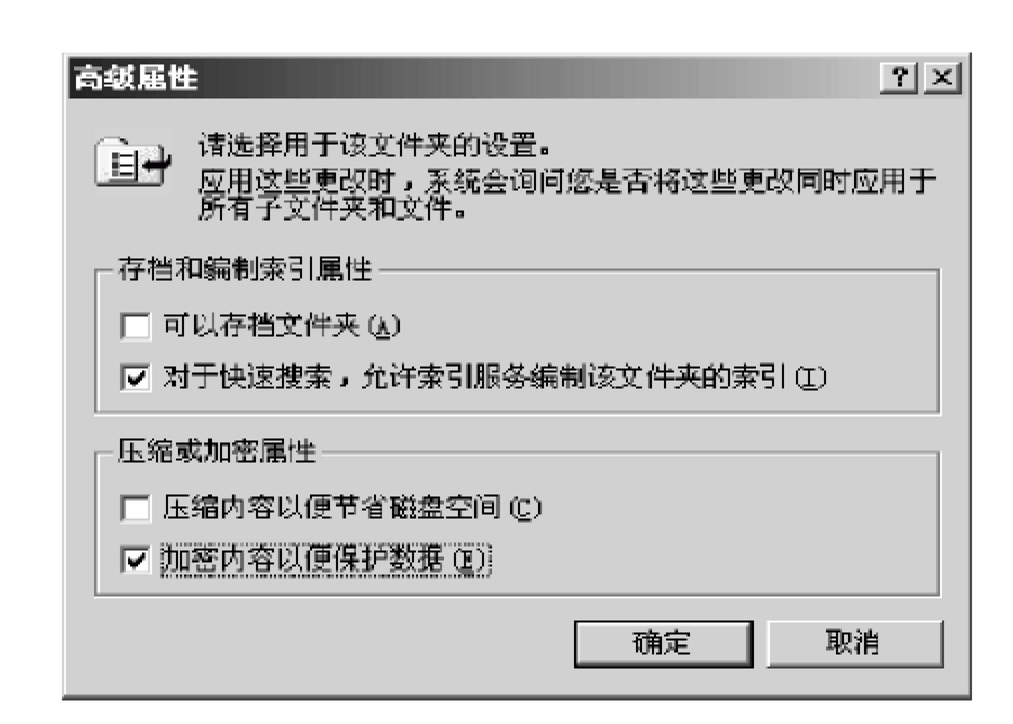


图 1.17 对文件夹加密属性进行设置

（4）注销用户重新登录后验证对 SecurityTest1 文件夹的读取权限。

6. 实验报告与要求

根据上面介绍的各项安全性实验要求，详细观察记录设置前后系统的变化，给出分析报告。

7. 实验分析与讨论

当前用户对文件夹进行 EFS 加密处理后，其他用户将无法打开查看。当需要将加密文件夹授权给其他用户时，可以由加密文件夹的用户为当前的加密文件系统 EFS 设置证书，并将证书导出，由被授权用户导入自己帐户的 EFS 系统。实验者可自行探索操作方法。

8. 注意事项

进行各设置项目验证时，注意用户的切换。

1.2.4　服务管理

1. 实验目的

了解服务管理功能并掌握其设置方法。

2. 实验原理

Windows 中有许多用不着的服务处于激活状态，它们中可能存在的安全漏洞使攻击者甚至无需帐户就能控制机器。为了系统的安全，应关闭系统中用不到的服务，使系统提供的服务最小化。各服务项目都有其特定的功能，应进行相应了解后并根据用户的使用需要进行设置。同时，还要注意服务间是相互关联的，对操作对象应了解其依赖及被依赖的其他服务，避免影响计算机的正常使用。

3. 实验环境

一台安装 Windows 2000/XP 操作系统的计算机。

4. 实验内容

（1）关闭如下所有不需要的服务。

- Alerter(disable)
- ClipBook Server(disable)
- Computer Browser(disable)
- DHCP Client(disable)
- Directory Replicator(disable)
- FTP publishing Service(disable)
- License Logging Service(disable)
- Messenger(disable)

- Netlogon(disable)
- Network DDE(disable)
- Network DDE DSDM(disable)
- Network Monitor(disable)
- Remote Access Server(disable)
- Remote Procedure Call(RPC)locater(disable)
- Schedule(disable)
- Server(disable)
- Simple Services(disable)
- Spooler(disable)
- TCP/IP Netbios Helper(disable)
- Telephone Service(disable)

(2) 设置如下服务为手动启动。

- SNMP service(optional)
- SNMP trap(optional)

(3) 设置如下服务为自动启动。

- Eventlog(required)
- NTLM Security Provider(required)
- RPC Service(required)
- WWW(required)
- Workstation(leave service on: will be disabled later in the document)

5. 实验步骤

(1) 启动"管理工具"|"服务",选中相应服务项目右击打开属性对话框进行设置,如图 1.18 和图 1.19 所示。

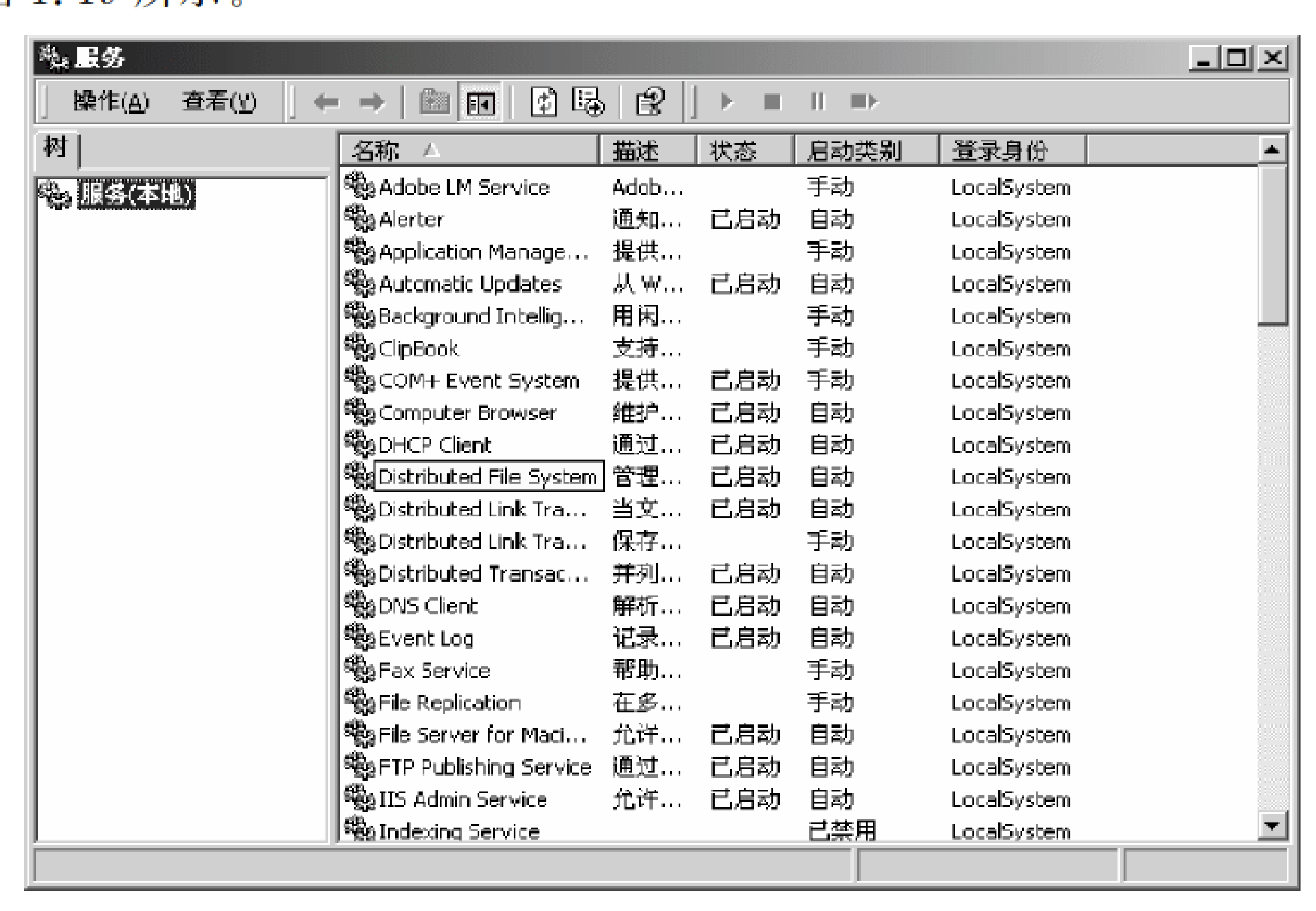


图 1.18 对系统服务项目进行设置



图 1.19　对系统服务项目属性进行设置

(2) 手动启动服务，在命令行窗口输入 net start [service]启动服务，net stop[service]关闭服务，如图 1.20 所示。

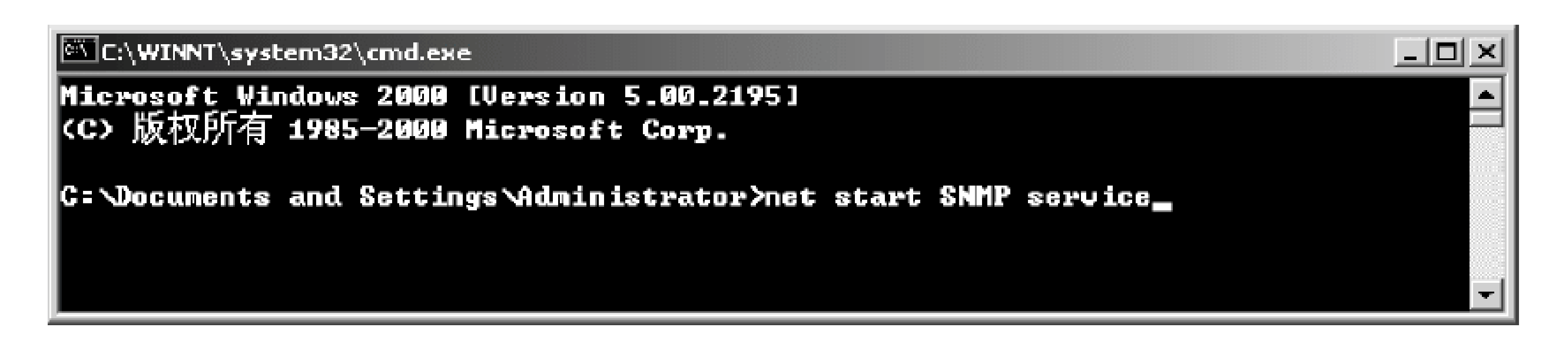


图 1.20　手动方式设置服务属性

6. 实验报告与要求

根据上面介绍的各项安全性实验要求，详细观察记录设置前后系统的变化，给出分析报告。

7. 实验分析与讨论

进行服务的属性设置时，需要考虑系统的可用性、系统的运行效率和安全性，同时还要考虑各服务项间的相互依赖性，读者可进一步思考如何确定合理的服务设置方案。

8. 注意事项

各项服务的功能和相互关系可查阅相关帮助文档。不同 Windows 系统中的服务条目略有不同。

1.2.5 端口安全

1. 实验目的

了解端口与服务的对应关系并掌握端口的设置方法。

2. 实验原理

为减少可能的系统入侵途径，提高系统安全性，应只开放服务需要的端口与协议，而关闭其他用不到的端口。常用的 TCP 端口有 80(Web 服务)、21(FTP 服务)、25(SMTP)、23(Telnet)、110(POP3)等；常用的 UDP 端口有 53(DNS 域名解析服务)、161(SNMP)、8000/4000(OICQ)等。

3. 实验环境

一台安装 Windows 2000/XP 操作系统的计算机。

4. 实验内容

(1) 打开 TCP 协议的 80 端口(只提供 HTTP 服务)，并对控制效果进行验证；
(2) 打开 TCP 协议的 21 端口(只提供 FTP 服务)，并对控制效果进行验证。

5. 实验步骤

(1) 打开"网络"|"本地连接"|"属性"|"Internet 协议(TCP/IP)"|"属性"|"高级"|"选项"|"TCP/IP 筛选"|"属性"，启用"TCP/IP 筛选"。
(2) 依次在 TCP 端口中添加 21 和 80 端口，如图 1.21 所示。

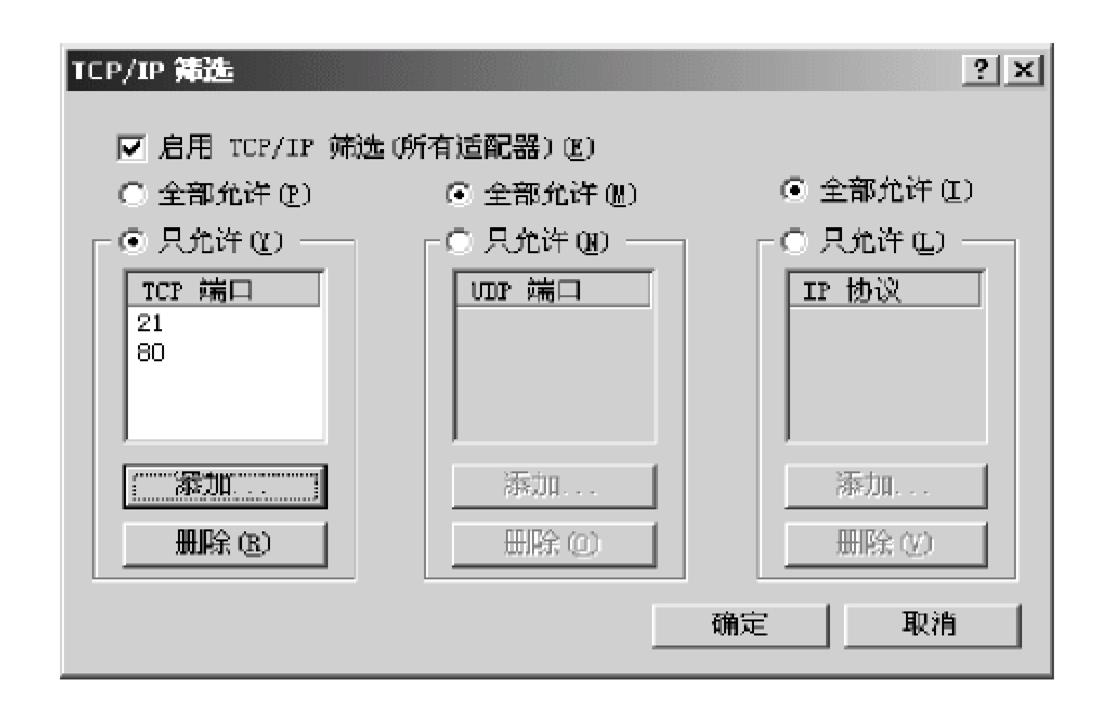


图 1.21 系统端口选项设置

6. 实验报告与要求

根据上面介绍的各项安全性实验要求，详细观察记录设置前后系统的变化，给出分析报告。

7. 实验分析与讨论

进行本实验时，实验小组成员可以相互配合，结合本地 HTTP 和 FTP 服务的提供，验证端口设置的有效性。

8. 注意事项

在该窗口中进行设置时，采用的是最小特权原则，所添加的为开放端口，其他端口全部禁用。

1.2.6　IIS 服务安全设置

1. 实验目的

通过实验了解 Windows 操作系统中 IIS 服务的安全漏洞及其防范措施，实现 Web 和 FTP 服务器的安全配置。

2. 实验原理

IIS(Internet Information Server)是 Windows 系统中的 Internet 信息和应用程序服务器。利用 IIS 可以配置 Windows 平台方便地提供各种应用。IIS 4.0 和 IIS 5.0 的应用非常广泛，但这两个版本均存在很多漏洞，它们的使用也带来了很多安全隐患。因此，了解如何加强 Web 服务器、FTP 服务器的安全性，防范由 IIS 漏洞造成的入侵非常重要。

为保护 Windows 2000 Server 系统的安全性，应删除默认的站点，重新建立自己的站点，并将 IIS 与系统安装在不同的分区，可以避免 IIS 安全漏洞直接威胁到系统的安全。

3. 实验环境

一台安装有 Windows 2000 Server 操作系统的主机。

4. 实验内容

(1) 启用 IIS 服务；

(2) 关闭并删除默认 FTP 和 Web 站点；

(3) 建立自己的站点，并确保对应目录的访问控制权限为 Administrator(完全控制)，System(完全控制)；

(4) 维护站点的安全日志；

(5) 设置拒绝如下 IP 地址的 FTP 访问。单机：192.168.0.60；网段：标识——202.120.110.1，子网掩码——255.255.255.0。

5. 实验步骤

(1) 打开"开始"|"设置"|"控制面板"，单击"添加/删除程序"，选择左边的"添加/删除 Windows 组件"，然后按照屏幕提示安装 IIS 组件，如图 1.22 所示。

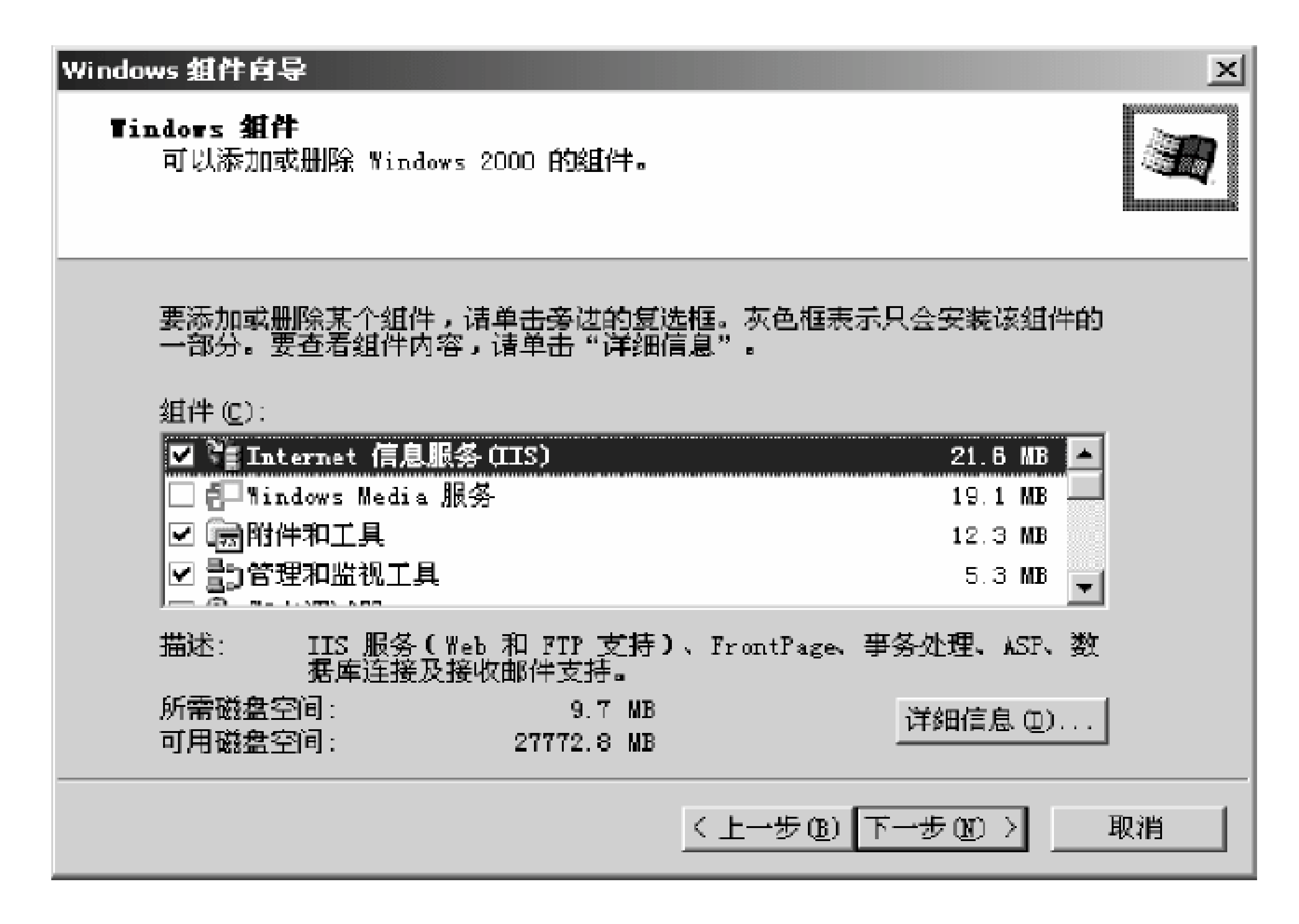


图 1.22 安装 IIS 组件

(2) 在"管理工具"|"Internet 服务管理器"中选中默认 FTP 站点和默认 Web 站点，右击"删除"选项，如图 1.23 所示。



图 1.23 删除默认 Web 站点和 FTP 站点

(3) 新建自己的 FTP 和 Web 站点，并将目录文件夹设置在其他磁盘上，如图 1.24 和图 1.25 所示。

(4) 设置 Web 站点基本属性，如图 1.26 和图 1.27 所示。



图 1.24　新建自己的 Web 站点



图 1.25　设置 Web 站点目录

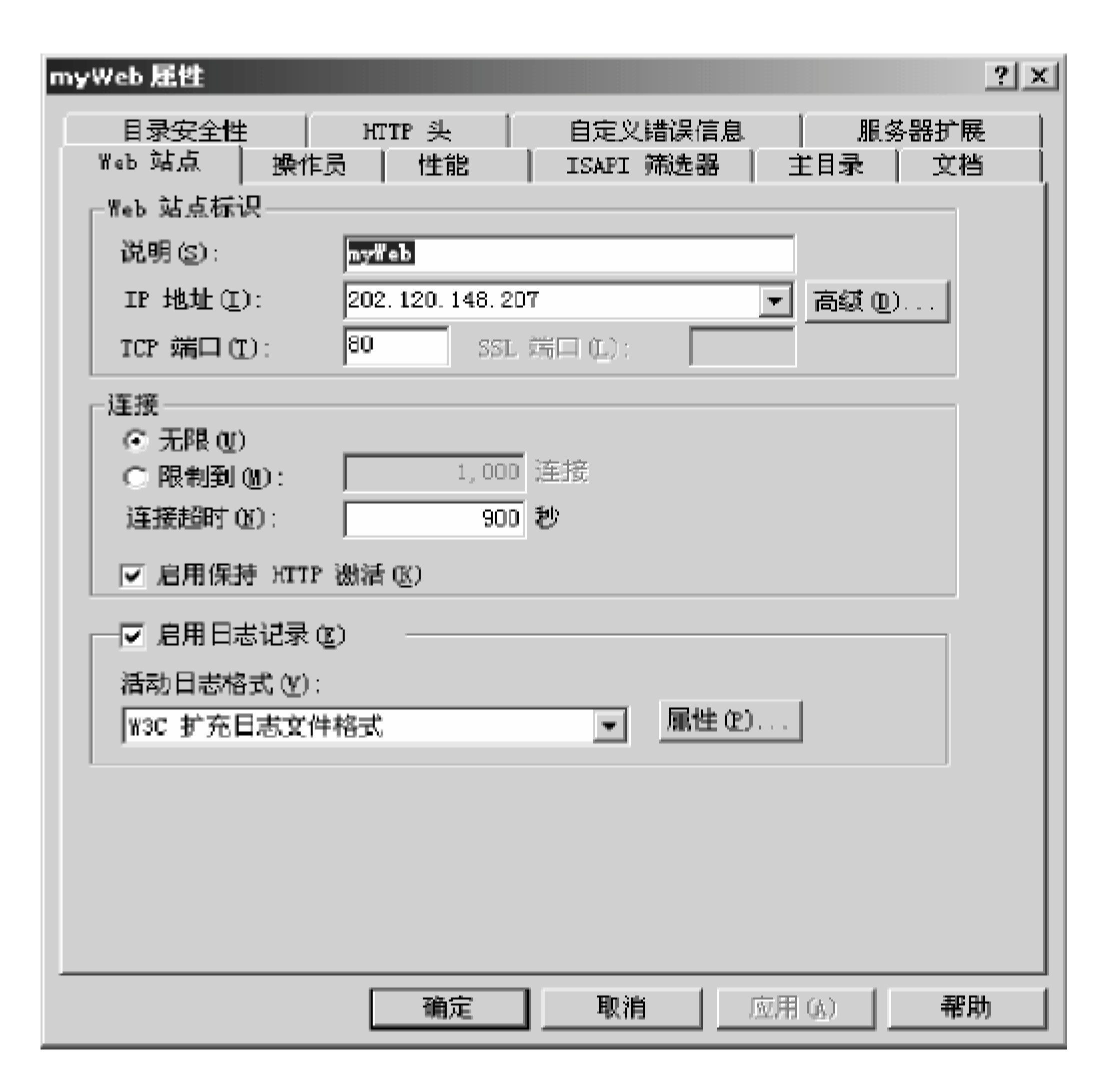


图 1.26　设置 Web 站点基本属性

(5) 创建自己新的 FTP 站点,在"安全帐号"选项卡中进行设置,如图 1.28 所示。



图 1.27 设置 Web 站点日志属性

图 1.28 设置 FTP 站点帐号属性

(6) 在"目录安全性"选项卡中进行设置,如图 1.29 和图 1.30 所示。

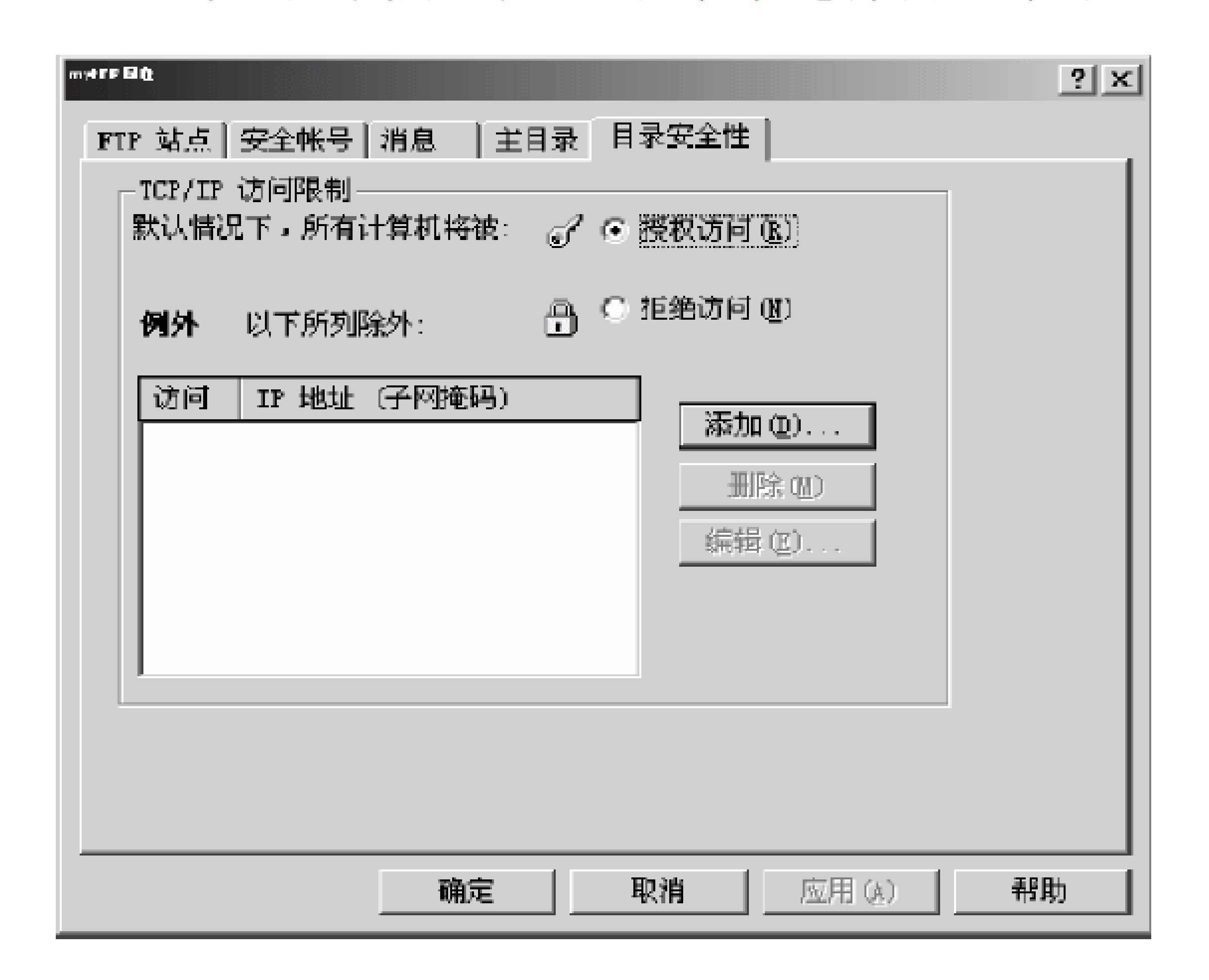


图 1.29 设置 FTP 站点访问属性(1)



图 1.30 设置 FTP 站点访问属性(2)

6. 实验报告与要求

根据上面介绍的各项安全性实验要求,详细观察记录设置前后系统的变化,给出分析报告。

7. 实验分析与讨论

对于 Web 和 FTP 站点,还有其他设置项目,如限制 FTP 服务器的操作员,对主目录的访问权限控制,修改相应的端口地址等。读者可以在站点属性窗口的各选项卡中进行配置。

8. 注意事项

除了主目录应与系统文件分开存放外，日志文件也应存放在和主目录不同的路径下，并设置访问权限，以保护日志文件的安全性。

1.2.7　系统备份与恢复

1. 实验目的

了解 Windows 提供的备份与恢复功能，掌握对系统和用户数据进行备份和恢复的方法。

2. 实验原理

即使熟练地配置了各种安全产品，灾难也可能会发生，数据备份可以在数据被销毁或者被破坏时找回数据，因此是最重要的安全措施之一。

备份应该定期执行。备份方法分为完整备份、差异备份和增量备份等。完整备份会复制所有指定的文件，占用的时间最长，但可以最快地恢复。差异备份将会复制上次完整备份后，所有曾被改变的文件，如果要复原整个系统，则要先复原完整备份，再复原最后一次的差异备份，所以会占用较长的时间，因为将有两个媒体要恢复。增量备份将会备份最后一次备份以来新增的数据（包括完整备份或增量备份）。备份数据应该被保存在远程场所，以使它们免于火灾或计算机附近的一些其他局部环境问题的危害。

3. 实验环境

一台安装 Windows 2000/XP 操作系统的计算机。

4. 实验内容

（1）新建文件夹 SecurityTest，对该文件夹和系统状态数据进行备份并进行还原操作练习；

（2）制订一份系统备份计划并进行设置；

（3）为自己的计算机制作一份系统紧急修复盘；

（4）利用注册表工具对注册表进行备份并进行导入导出练习。

5. 实验步骤

（1）启动“程序”|“附件”|“系统工具”|“备份”中的“备份”选项卡，选中需要备份项目，依次进行备份设置，完成后再进行还原操作，如图 1.31 所示。

（2）在备份计划中按照提示进行计划制订，如图 1.32 所示。

（3）选中“欢迎”选项卡，启动“紧急修复磁盘”，如图 1.33 所示。



图 1.31　进行系统备份设置



图 1.32　制订备份计划

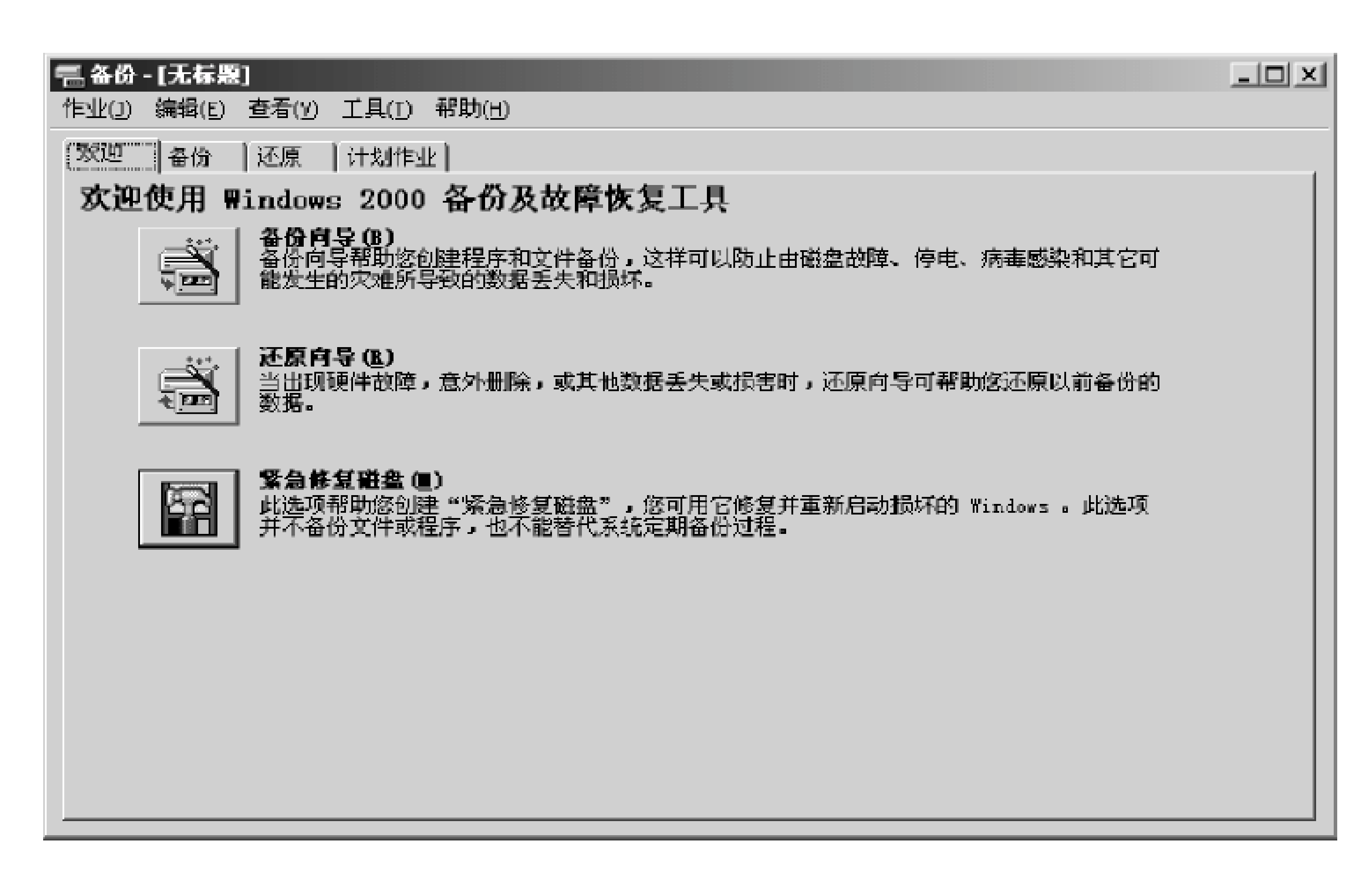


图 1.33　制作系统紧急修复磁盘

(4) 选择“程序”|“运行”命令，在“运行”对话框中输入 regedit，打开注册表，在“注册表”菜单中进行导入导出练习，如图 1.34 所示。



图 1.34　管理系统注册表

6. **实验报告与要求**

根据上面介绍的各项安全性实验要求，详细观察记录设置前后系统的变化，给出分析报告。

7. **实验分析与讨论**

除了使用系统自带的数据备份恢复工具外，还可以使用其他一些工具，如 Ghost 软件。Ghost 以硬盘的扇区为单位进行物理信息的完整复制。对于误格式化、误删除引起的数据丢失，只要没有向丢失数据所在的分区上写入新的数据，就可以利用 FinalData 等数据恢复软件实现接近 100%的恢复。因为在 Windows 环境下删除一个文件，只有目录信息从 FAT 或者 NTFS 删除，而文件数据仍然留在磁盘上。但是，如果开始使用的是专业的数据删除软件来删除数据，且覆盖了数据，就无法进行恢复了。

8. **注意事项**

(1) 备份数据将被存储于指定路径中的一个 kbf 文件中，数据恢复时则需要选中相应的 kbf 文件。

(2) 选中备份作业窗口中的“高级”按钮，可以选择具体的备份方式，如图 1.35 所示。

(3) 对注册表进行导入操作时，需要选中相应的 reg 文件，选中注册表某分支，可以实现注册表的部分导出。

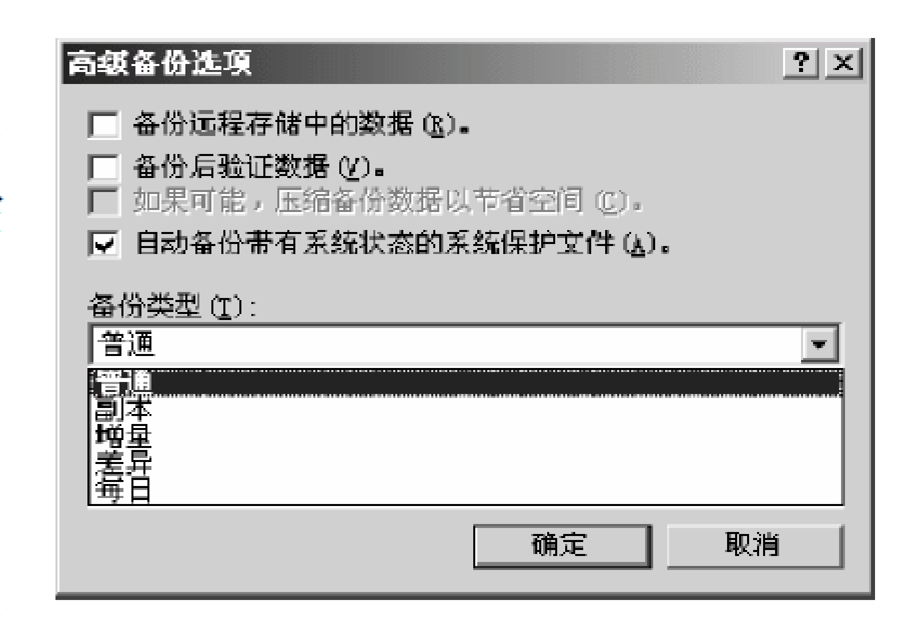


图 1.35　设置备份高级选项

第 2 章

网络安全

2.1 实验基础

2.1.1 网络通信安全基础

Internet 安全问题存在是由其自身的特征决定的：Internet 本身是没有边界的、全球的因特网，不属于任何一个组织或国家；通过 IP 地址来识别和管理存在严重的安全漏洞；Internet 本身没有中央管理机制，没有法令和法规，无法实现集中有效管理；Internet 从技术上来讲是开放的、标准的，缺乏一些安全防范机制；Internet 没有审计和记录的功能。

国内的网络安全现状尤为不容乐观。我国许多网络建网初期很少或根本没有考虑安全防范措施，相当大比例单位的计算机系统或多或少存在安全漏洞。我国目前极缺网络及电脑高级系统管理人员，高等教育中也较为缺乏这方面人才的培养，社会则缺乏造就这类人才的实践环境。另外，中国内地大部分网站是基于国外的产品，它们的安全系数令人怀疑。

2.1.2 常见网络攻击与防范技术

网络攻击的发起者通常被称为黑客。据统计国际上几乎每 20 秒就有一起黑客事件发生，仅美国每年由黑客所造成的经济损失就超过 100 亿。

常见黑客攻击过程包括如下几个步骤：

(1) 目标探测和信息收集：确定攻击目标并收集目标系统的有关信息，包含踩点、扫描、查点等几个步骤。

① 踩点：尽可能多地收集关于目标系统的安全状况的各个方面的信息；

② 扫描：使用各种工具和技巧确定哪些系统存活着，它们在监听哪些端口、操作系统等，确定入攻途径。

③ 查点：从系统中抽取有效帐号或导出资源名的过程。

(2) 获得访问权：通过密码窃听、共享文件的野蛮攻击、攫取密码文件并破解或缓冲区溢出等攻击来获得系统访问权限；

(3) 特权提升：一般帐户对目标系统只有有限的访问权限，黑客经常会通过采用密码

破解、利用已知漏洞等方法来获得更高权限；

(4) 掩踪灭迹：一旦目标系统已全部控制，黑客便会隐藏自己的踪迹，防止被管理员发觉；

(5) 创建后门：在系统的不同部分布置陷阱和后门，以便入侵者在以后仍能获得特权访问。

常见的网络攻击技术有IP欺骗与防范、Sniffer嗅探器、端口扫描技术、特洛伊木马、拒绝服务式攻击等。

1. IP欺骗与防范

一台主机使用的不是分配给自己的IP地址的现象属于IP地址盗用。IP地址盗用是一种常见问题，不需编程即可进行。盗用IP应该是只能盗用本网段的IP，因为最简单的网段也要有一个路由器作为出口。在路由器的配置中，要制定这个网段的网络地址和掩码。如果该网段中的主机使用了其他网段的IP，则路由器不认为属于它的网段，不给转发。

防止盗用IP可以绑定IP和物理地址。通过设置路由器上的静态ARP(地址转换协议，将硬件地址与IP地址相关联的协议的一部分)表，可防止在本网段内盗用IP。

IP电子欺骗指伪造某台主机的IP地址的技术。被伪造的主机往往具有某种特权或者被另外的主机所信任，通常要用编写的程序实现，通过发送带有假冒的源IP地址的IP数据包，来达到自己的目的，以IP地址验证为基础。IP电子欺骗出现的可能性较小，一般使用防火墙可以很容易地防备这种攻击方法。应确信只有内部网络可以使用信任关系，并在路由器设置不允许声称来自于内部网络的外来包通过。

2. Sniffer嗅探器

以太网工作原理是基于总线方式，一台机器发给另一台机器的数据，共享hub先收到，然后把它接收到的数据再发送给其他所有的端口，共享hub连接的同一网段的所有机器的网卡都能收到数据，使得两台机器传输数据时别的端口也被占用了，因此同一网段同一时间只能有两台机器进行数据通信。网卡收到传输来的数据，网卡内的固化程序先接收数据头的目的MAC地址，判断是否与自己的地址相同，如果相同，就接收下来存在网卡的缓冲区中，然后产生中断信号通知CPU，如果不同就丢弃。CPU得到中断信号后产生中断，操作系统根据网卡驱动程序设置的网卡中断程序地址调用驱动程序接收数据，放入堆栈让操作系统处理。

当发送者希望引起网络中所有主机操作系统的注意时，他就使用“广播地址”。多数网络接口具有设置成“混杂方式”的能力。在混杂方式下，网络接口对遭遇到的每一帧都产生一个硬件中断，而不仅仅是针对目标为自己硬件地址或“广播地址”的帧。窥探仪通常将网络接口设置成混杂方式以便监视网段内的每一个数据报文。Sniffer嗅探器通知网卡接收其收到的所有数据(混杂模式)，并通知主机进行处理。如果发现感兴趣的包或是符合预先设定的过滤条件的包(如设定包中包含username或password、银行卡卡号、金融信息等)，就将其存到一个log文件中。Sniffer通常运行在路由器或有路由器功能的主机上，使得可以对大量的数据进行监控。Sniffer属于数据链路层的攻击，通常攻击者已经进入了目标系统。

Sniffer可以通过查找异常进程来发现。为防止Sniffer，可以为传输加密，根本方法是增强TCP/IP协议。目前阶段基本是通过打补丁来解决，如SSH协议和F-SSH协议。另

外一种防范措施是采用安全拓扑结构。一个网络段必须有足够的理由才能相信另一网络段。网络段的设计应该考虑数据之间的信任关系,而不是硬件需要,将所有的问题都归结到信任上。计算机和其他计算机通信,必须信任这台计算机。考虑信任关系路径的长度,尽可能使得 Sniffer 出现后,只对最小范围有效。Sniffer 往往是攻击者侵入系统后才使用,因此防止系统被突破是关键。

3. 端口扫描技术

TCP/IP 协议为每种服务设定了一个端口。每个端口拥有一个 16 位的端口号(一台主机可以定义 2^{16} 即 65 536 个端口)。用户自己提供的服务可以使用自由端口号。一般系统使用的端口号是 0～1023,用户自己定义的端口号从 1024 开始。TCP/IP 服务一般通过 IP 地址加一个端口号 Port 来决定。客户端程序一般通过服务器的 IP 地址和端口号与服务器应用程序进行连接(WWW 80, FTP 21, SMTP 25, POP3 110)。端口就是一个潜在的通信通道或入侵通道。对目标计算机进行端口扫描,能得到许多有用的信息,从而发现系统的安全漏洞。可以手工或通过端口扫描软件来扫描端口。

与手工扫描相关的网络命令有以下几个:

(1) ping:可以检测网络目标主机存在与否以及网络是否正常(能否通达)。

(2) tracert:用来跟踪一个报文从一台计算机到另一台计算机所走的路径。

(3) finger:显示用户的状态,如用户名、登录的主机、登录日期等。

(4) rusers:显示远程登录的用户名、该用户的上次登录时间等。

(5) hosts:可以收集到一个域里所有计算机的重要信息,包括域里名字服务器的地址,一台计算机上的用户名,一台服务器上正在运行什么服务及这个服务是哪个软件提供的,计算机上运行的是什么操作系统等。

扫描器是一种自动检测远程或本地主机安全性弱点的程序。它的工作原理是通过选用远程 TCP/IP 不同端口的服务,记录目标给予的回答来实现。扫描器不是一个直接攻击网络漏洞的程序,它仅仅帮助入侵者发现目标主机的某些内在弱点。好的扫描器会对它得到的数据进行分析,帮助入侵者查找目标主机的漏洞,但不会提供进入一个系统的详细步骤。其基本功能包括:发现一个主机或网络;发现该主机正在运行的服务;通过测试这些服务,发现内在的漏洞。

4. 特洛伊木马

特洛伊木马(trojan horse)是一个程序,它驻留在目标计算机里。在目标计算机系统启动的时候,特洛伊木马自动启动,然后在某一端口进行侦听。如果在该端口收到数据,对这些数据进行识别,然后按识别后的命令,在目标计算机上执行一些操作,如窃取口令、复制或删除文件、重启计算机等。攻击者一般在入侵某个系统后,想办法将特洛伊拷贝到目标计算机中,并设法运行这个程序,从而留下后门。以后,通过运行该特洛伊的客户端程序,对远程计算机进行操控。

木马与病毒的区别在于木马不具备复制能力。木马的运行应该符合三个条件:

(1) 木马需要一种启动方式,一般在注册表启动组中;

(2) 木马需要在内存中运行才能发挥作用;

(3) 木马会占用一个端口,以便黑客通过这个端口和木马联系。

木马具有隐蔽性、顽固性、潜伏性等特点。

要发现和删除木马,可以采取下面的方法:

(1) 发现木马:使用端口扫描软件,查看是否有可疑的端口开放。如有则先记下该端口号,然后查看内存中正在运行的软件,记录其名称和硬盘位置,并依次终止。如果端口依然开放,则被终止的程序不是木马,继续终止,直到发现木马。

(2) 删除方法:备份需要删除的文件和注册表;终止程序在内存中的运行;在注册表中查询包含该文件名的键值,然后删除。对于捆绑式木马,重新安装被捆绑程序。删除木马最简单的方法是安装杀毒软件。

5. 拒绝服务式攻击

DoS(Denial of Service)攻击行动使网站服务器充斥大量要求回复的信息,消耗网络带宽或系统资源,导致网络或系统不胜负荷以致瘫痪而停止提供正常的网络服务。

拒绝服务式攻击的原理为:发送者发出“我来了”的连接请求后,立即离开。服务器收到请求却找不到发送该请求的客户端。于是,按照协议,它等一段时间后再与客户端连接。用户传送众多要求确认的信息到服务器,使服务器里充斥着这种无用的信息。所有的信息都有需要回复的虚假地址,以至于当服务器试图回传时,却无法找到用户。服务器于是暂时等候,然后再切断连接。用户再度传送新一批需要确认的信息,周而复始,导致服务器无法正常工作,完全瘫痪。

DDoS(Distributed Denial of Service,分布式拒绝服务攻击)的工作原理为攻击者利用上千台客户端同时攻击一个服务器。其攻击步骤为:

(1) 探测扫描大量主机以寻找可入侵目标主机;

(2) 入侵有安全漏洞的主机并获得控制权;

(3) 在每台入侵主机中安装攻击程序;

(4) 利用已入侵主机继续扫描和入侵。

防范拒绝服务式攻击,首先要防止成为被利用的工具,其次要防止成为被攻击的对象。可以采取的防范措施有:

(1) 优化路由及网络结构;

(2) 优化对外提供服务的主机。使用多宿主机,将网站分布在多个不同的物理主机上,防止网站在遭受攻击时全部瘫痪;

(3) 当攻击正在进行时,立即启动应付策略,尽可能快地追踪攻击包,并与服务提供商联系;

(4) 提高系统安全强度,防止被入侵。如经常下载系统软件补丁,开启尽可能少的服务,对系统进行安全审核、漏洞排查等。

2.1.3 防火墙技术

防火墙是综合采用适当技术,通过对网络做拓扑结构和服务类型上的隔离,在被保护网络周边建立的分隔被保护网络与外部网络的系统。它通常是软件和硬件的组合体。

防火墙适合在专网中使用,特别是在专网与公共网络互联时。它所保护的对象是网络中有明确闭合边界的一个网块,它的防护对象是来自被保护网块外部的对网络安全的威胁。

防火墙一般具有以下基本功能：

（1）过滤进出网络的数据包；

（2）管理进出网络的访问行为；

（3）封堵某些禁止的访问行为；

（4）记录通过防火墙的信息内容和活动；

（5）对网络攻击进行检测和警告。

防火墙的优点有：

（1）简化安全管理；

（2）保护网络中脆弱的服务；

（3）用户可以很方便地通过审计监视网络的安全性，并产生报警信息；

（4）增强保密性，强化私有权；

（5）防火墙是审计和记录网络流量的一个最佳地方。

防火墙的缺陷有：

（1）限制有用的网络服务；

（2）不能有效防护内部网络用户的攻击；

（3）Internet 防火墙无法防范通过防火墙以外的其他途径的攻击；

（4）防火墙也不能完全防止传送已感染病毒的软件或文件；

（5）防火墙无法防范数据驱动型（表面上看是没有害处的数据，而其中隐藏了一些可以威胁主机安全的指令）的攻击；

（6）不能防备新的网络安全问题。防火墙是一种被动式的防护手段，只能对现在已知的网络威胁起作用。

防火墙的类型有包过滤型防火墙、双宿网关防火墙和屏蔽子网防火墙。

包过滤型防火墙又称网络级防火墙。包过滤型防火墙一般通过路由器实现，也称作包过滤路由器（packet filtering router）。包过滤防火墙工作原理为在网络层对进出内部网络的所有信息进行分析，并按照一组安全策略（信息过滤规则）进行筛选，允许授权信息通过，拒绝非授权信息。信息过滤规则以收到的数据包的头部信息为基础。过滤路由器基于源 IP 地址、目的地址和 IP 选项进行过滤。包过滤型防火墙遵循“最小特权原则”，即明确允许管理员希望通过的数据包，禁止其他的数据包。

包过滤型防火墙的优点有：

（1）工作在网络层，根据数据包的报头部分进行判断处理，不去分析数据部分，因此处理包的速度比较快；

（2）实施费用低廉，一般的路由器已经内置了包过滤功能；

（3）包过滤路由器对用户和应用来讲是透明的，用户可以不知道包过滤防火墙的存在，也不需要对客户端进行变更；不需特别的培训和安装特定的软件。

包过滤型防火墙有以下缺点：

（1）定义数据包过滤规则会比较复杂；

（2）只能阻止一种类型的 IP 欺骗，即外部主机伪装内部主机的 IP，不能防止外部主机伪装其他可信任的外部主机的 IP；

（3）直接经由路由器的数据包都有被用作数据驱动型攻击的潜在危险；

（4）不支持基于用户的认证方式（网络层之上）；

（5）不能提供有用的日志；路由器本身存储容量有限；

（6）随着过滤规则的复杂化和通过路由器进行处理的数据包数目的增加，路由器的吞吐量会下降；

（7）IP 包过滤无法对网络上流动的信息提供全面的控制；无法对数据包正文部分进行分析。

双重宿主主机防火墙，是一种拥有两个连接到不同网络上的网络接口的防火墙。其特点是，内部网络与外部不可信任的网络之间是隔离的，两者不能直接进行通信。双重宿主主机可以提供两种方式的服务：用户直接登录到双重宿主主机，或在双重宿主主机上运行代理服务器。第一种方式管理困难，且危险性大（需要在宿主主机上建许多帐号，安全性差，不利管理）。因此，双宿主主机一般采用代理方式提供服务；该主机也称代理服务器（Proxy Server）。

双宿网关防火墙的原理为：首先要禁止网络层的路由功能，从而切断内外网络之间的 IP 数据流，同时强大的身份认证系统实现了访问控制。在网络层以上智能连接客户端和服务器，并能够检查 IP 包，加以分析，最终按照相应的内容采取相应的步骤。

代理服务器是接收或解释客户端连接并发起到服务器的新连接的网络节点。主要用于将企业网 Intranet 连接到 Internet。代理服务器分为应用层代理、传输层代理和 Socks 代理。代理服务器使用单个合法 IP 地址处理所有发出的请求。其优点有：

（1）节约合法的 C 类 IP 地址（最高位 110，网络号 21 位，主机号 8 位）；同时提高企业局域网的安全性，因为外部网络不能直接访问内部的私有 IP 地址；

（2）通过设置缓存能够加快浏览速度；

（3）具有较好的安全性，可以设置安全控制策略，提供认证和授权；

（4）可以根据用户名、源和目的地址及内容等进行过滤；

（5）具有强大的日志功能，并可进行流量计费。

双宿网关防火墙的缺点为：实现麻烦，每一种协议需要相应的代理软件（不支持代理的协议）；使用时工作量大，用户在受信任网络上通过防火墙访问 Internet 时，经常会出现延迟和多次登录才能访问外部网络的情况；速度较慢，不太适应于高速网之间的应用；内部用户对服务器主机的依赖性高。

屏蔽子网防火墙通过在内部网络和外部网络之间建立一个子网进行隔离。这个子网构造了一个屏蔽子网区域，称为边界网络（Perimeter Network），也称为非军事区（De-Militarized Zone，DMZ）。屏蔽子网防火墙系统使用了两个包过滤路由器：内部路由器、外部路由器和一个堡垒主机。将堡垒主机、信息服务器和其他公用服务器放在“非军事区”网络中，该网络很小，处于 Internet 和内部网之间。即使堡垒主机被入侵者控制，所能侦听到的内容也是有限的，即只能侦听到周边网络的数据，不能侦听到内部网上的数据。

屏蔽子网防火墙的“非军事区”配置成使用 Internet，内部网络系统能够访问“非军事区”网络上数目有限的系统，而通过“非军事区”网络直接进行信息传输是严格禁止的。外部路由器主要功能有：防范通常的外部攻击；管理 Internet 到 DMZ 的访问；通过代理服务只允许外部系统访问堡垒主机；保护“非军事区”上的主机。内部路由器功能有：负责管理 DMZ 到内部网络的访问；仅接收来自堡垒主机的数据包；完成防火墙的大部分过滤工作。一旦堡垒被控制，内部路由器仍可以对内部网络实施保护。堡垒主机的主要功能是进行安全防护；运行各种代理服务，如 WWW、FTP、Telnet。

屏蔽子网防火墙安全性好，但成本昂贵。

常见的防火墙产品有国外的 Check Point Firewall-1、Cisio PIX、Axent Raptor，国内的清华紫光、实达朗新等。

进行网络安全控制时需要先制定访问控制策略，访问控制策略规定了网络不同部分允许的数据流向，还会指定哪些类型的传输是允许的，哪些传输将被阻塞。访问控制描述符有：流向、服务、指定主机、用户个人、时间、加密与否、服务质量（如带宽限制）等。内容清楚的访问控制策略有助于保证正确选择防火墙产品。

设计和选用防火墙时，首先要明确哪些数据是必须保护的，这些数据的被侵入会导致什么样的后果，及网络不同区域需要什么等级的安全级别。其次，防火墙必须与网络接口匹配，要防止所能想到的威胁，防火墙自身应有相当高的安全保护。

好的防火墙应该是整个 Intranet 网络的保护者，而不局限于通过防火墙的使用者；能弥补操作系统之不足，为使用者提供不同平台的选择，并向使用者提供完善的售后服务。

2.2 实验项目

2.2.1 IE 浏览器安全设置

1. 实验目的

掌握 IE 浏览器提供的各项安全机制的配置方法，提高上网时的系统安全性。

2. 实验原理

IE 浏览器作为用户上网时的基本工具，提供了一系列基本的网络访问安全控制手段，用户应根据自己的需求进行重新设置，提高网络访问的安全性。

3. 实验环境

运行 Windows 操作系统的主机，安装 IE 6.0 软件。

4. 实验内容

（1）设置 Internet 安全选项，禁止下载未签名的 ActiveX 控件和未经安全认证的软件和插件；

（2）屏蔽 Cookies；

（3）添加 www.dhu.edu.cn 为可信站点，启用安全链接；

（4）添加 www.123.com 为受限站点；

（5）在个人信息中，禁用表单的自动完成功能，对表单和密码的自动完成历史记录进行清除；

（6）更改颜色显示，掩藏自己的上网访问痕迹；

（7）启用分级审查，设置监护人密码；

（8）通过以下方法恢复被修改的 IE 设置。

① 手工恢复被修改的主页：HKEY_CURRENT_USER、Software、Microsoft、Internet Explorer、Main。

② 利用软件工具恢复被修改的 IE 设置：如金山毒霸注册表修改工具或超级兔子系列软件。

5. 实验步骤

（1）选择“Internet 选项”|“安全”|Internet|“自定义级别”，分别选取相应的条目，如图 2.1 和图 2.2 所示。



图 2.1　设置 IE 安全级别

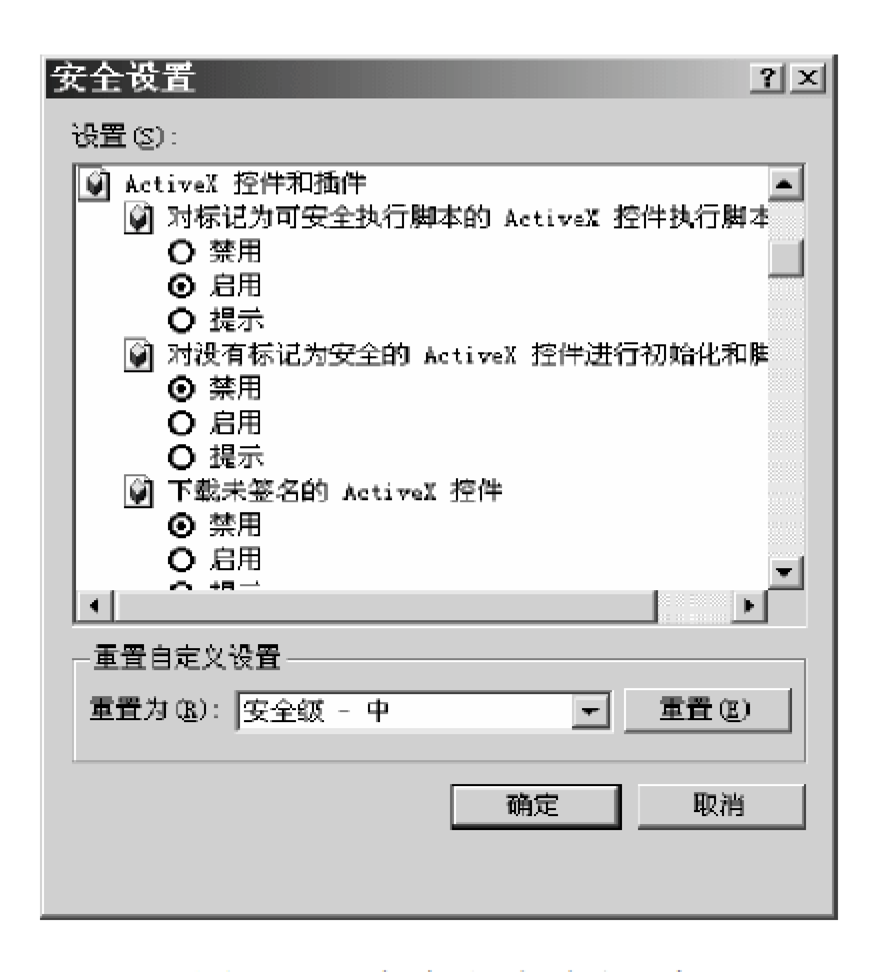


图 2.2　自定义安全级别

（2）选择“Internet 选项”|“隐私”选项卡，拖动滑块至最高级别，如图 2.3 所示。

（3）选择“Internet 选项”|“安全”|“受信任的站点”|“站点”，选中“对该区域中的所有站点要求服务器验证”复选框，输入 www.dhu.edu.cn 并添加，如图 2.4 和图 2.5 所示。



图 2.3　设置隐私保护级别

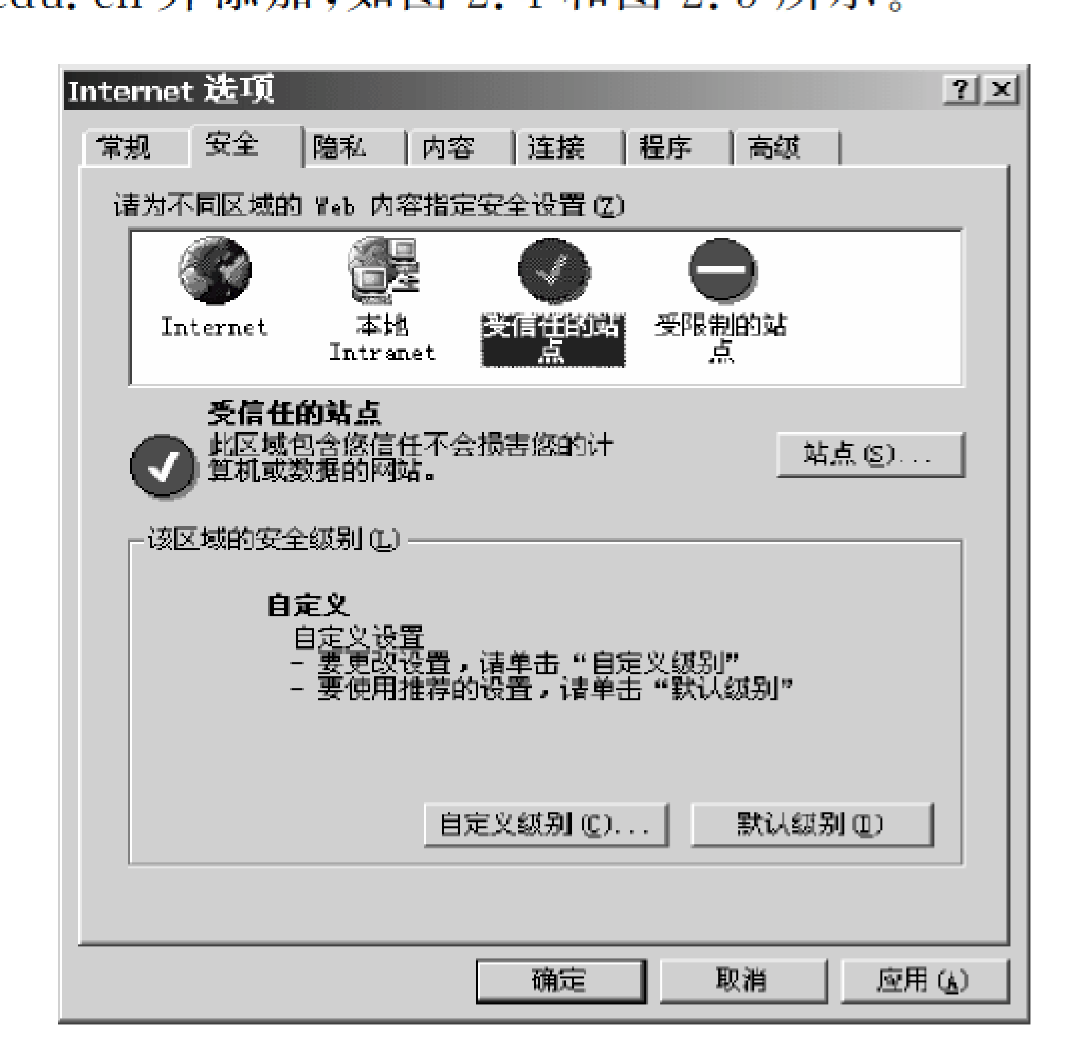


图 2.4　设置受信任站点

(4) 选择“Internet 选项”|“安全”|“受限制的站点”|“站点”,输入 www.123.com 并添加,如图 2.6 和图 2.7 所示。

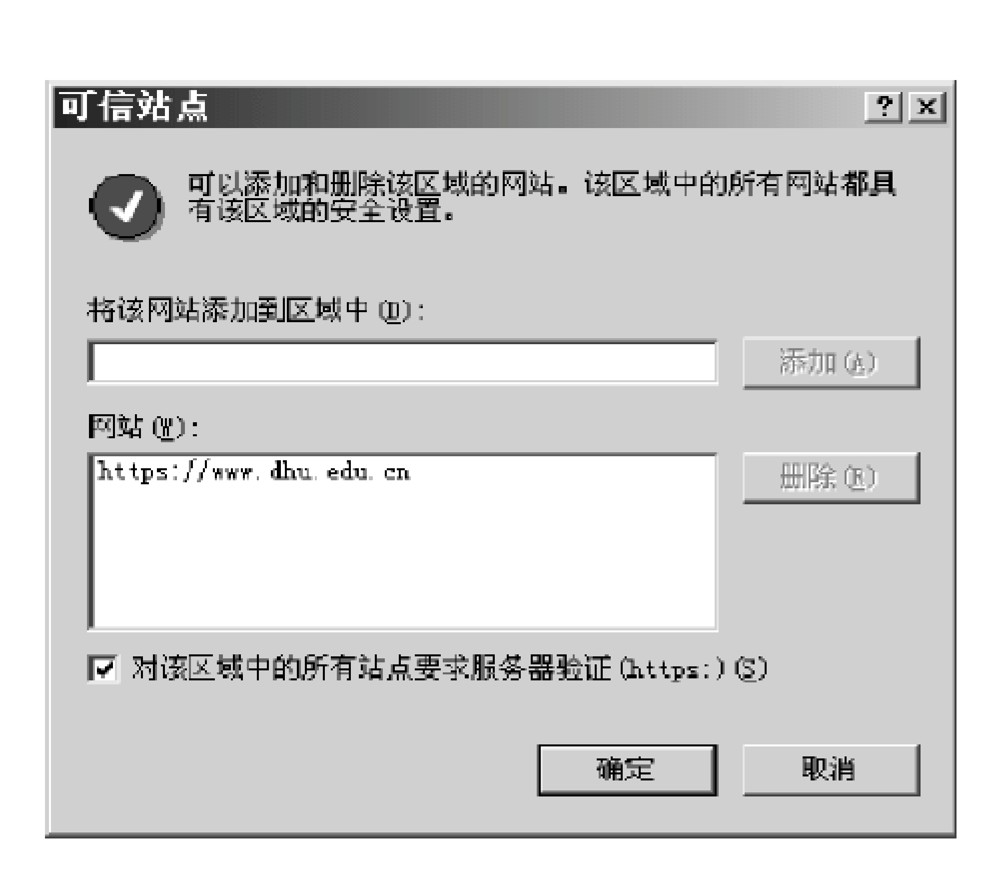


图 2.5 设置受信任站点信息



图 2.6 设置受限制站点

(5) 选择“Internet 选项”|“内容”|“个人信息”|“自动完成”,取消各选项,并单击“清除表单”、“清除密码”按钮,如图 2.8 所示。

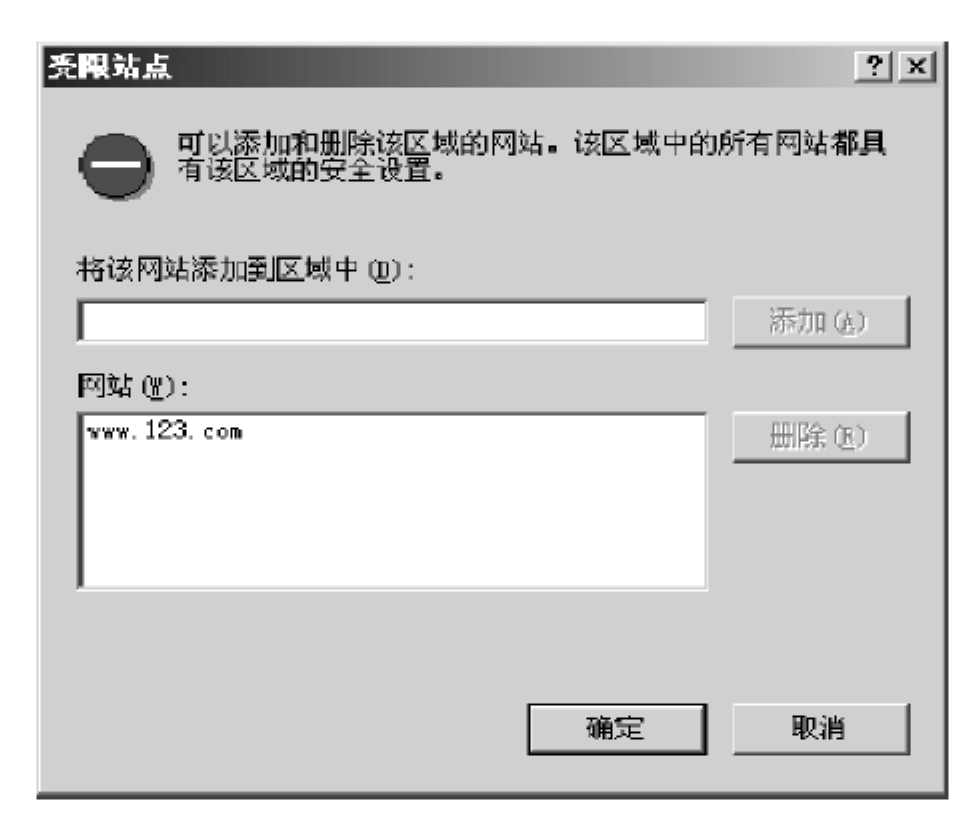


图 2.7 设置受限制站点信息



图 2.8 设置自动完成功能

(6) 选择“Internet 选项”|“常规”选项卡,单击“颜色”按钮,将访问过和未访问链接设为相同颜色;再单击“辅助功能”,选中“不使用网页中指定的颜色”复选框,如图 2.9 和图 2.10 所示。

(7) 选择“Internet 选项”|“内容”|“分级审查”|“设置”|“常规”,设置监督人密码,分别对审查内容进行定制,如图 2.11～图 2.13 所示。



图 2.9　设置网页显示颜色

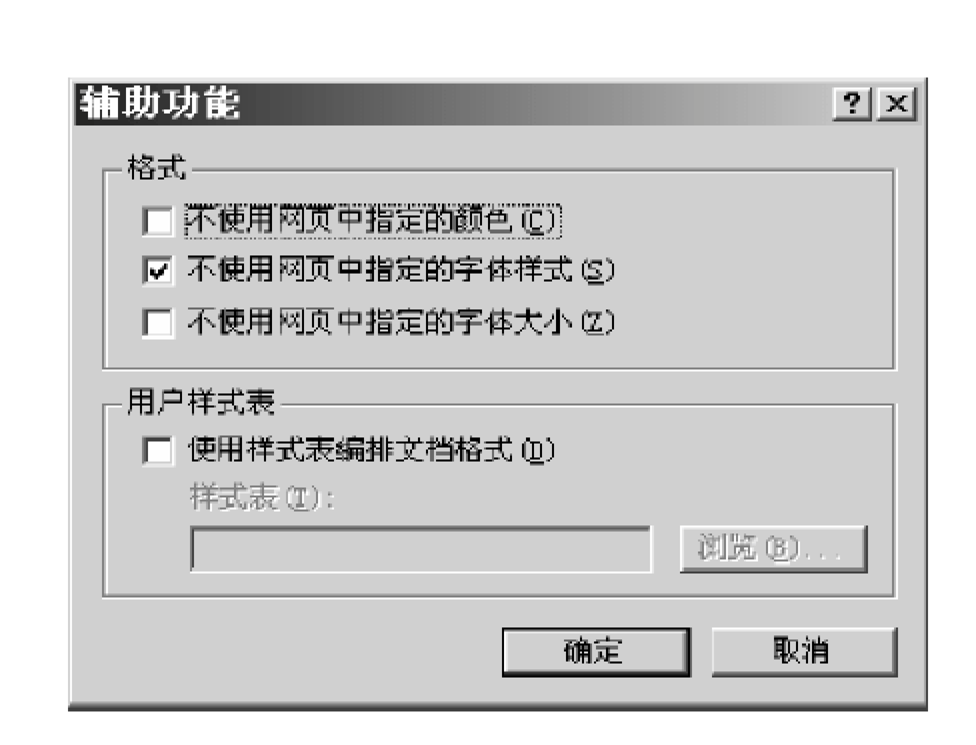


图 2.10　清除网页访问痕迹

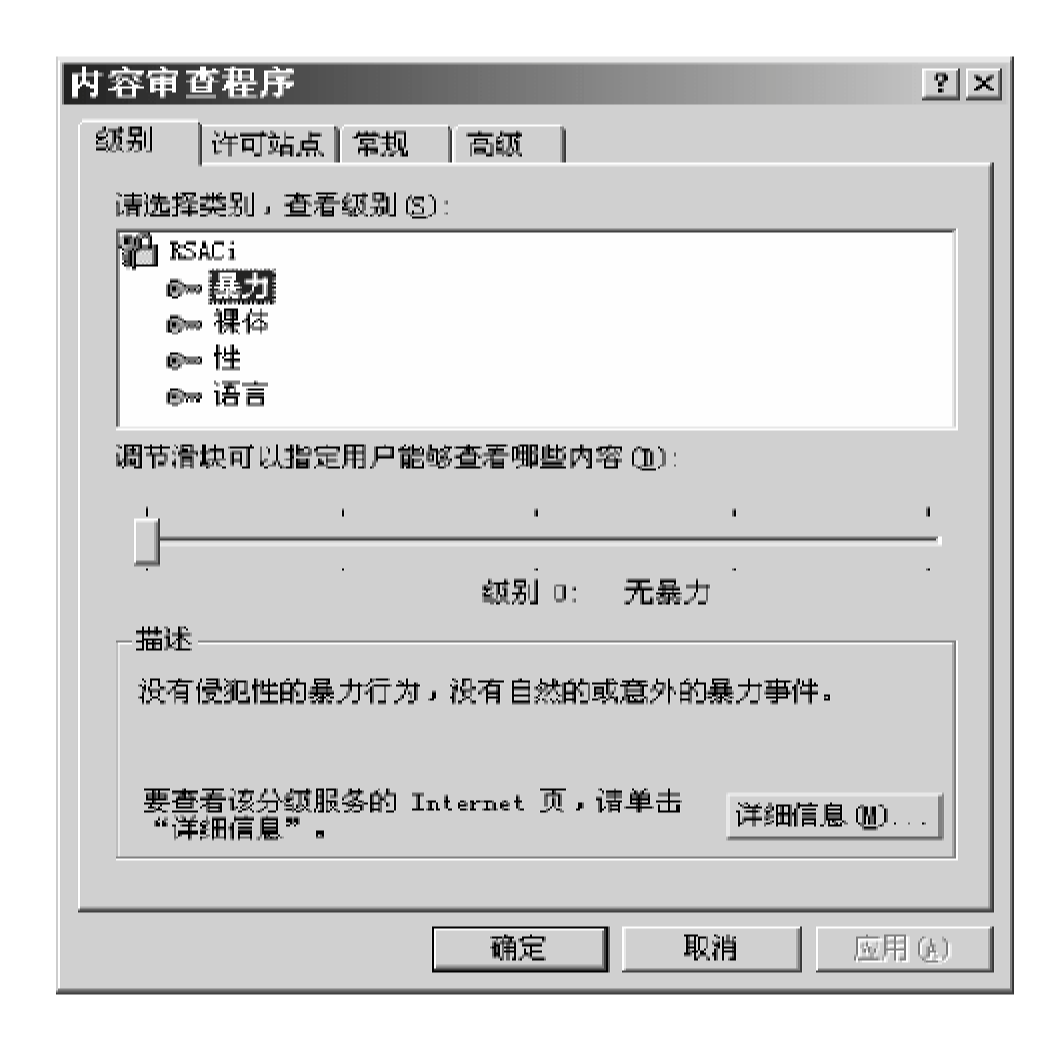


图 2.11　设置内容审查级别



图 2.12　设置监督人信息

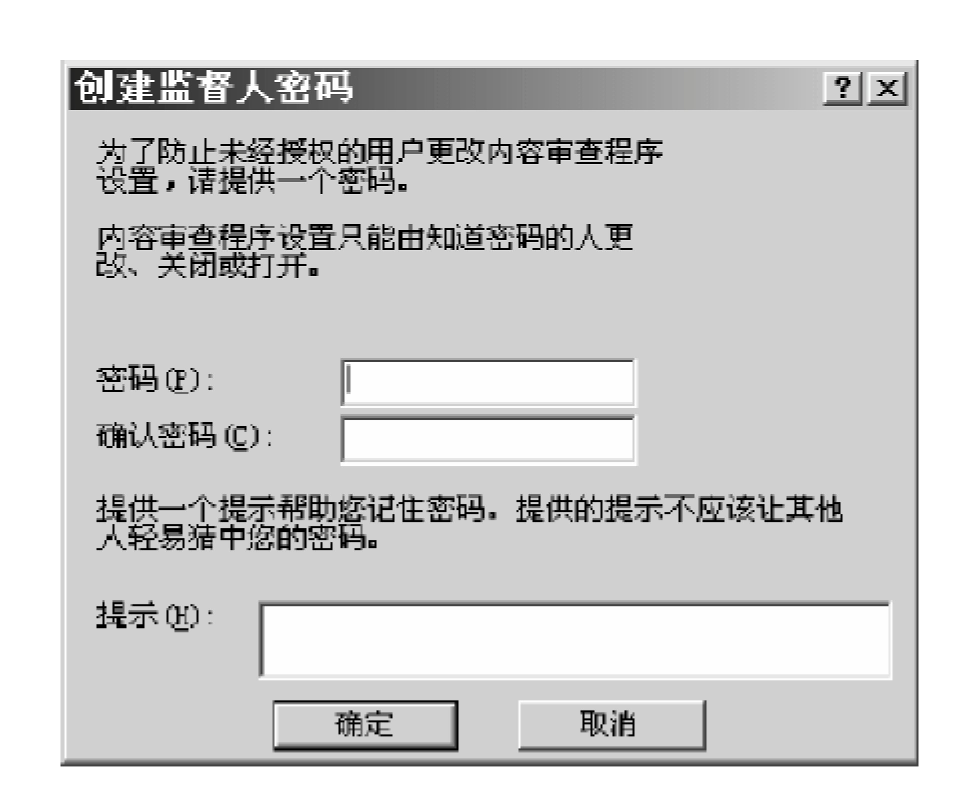


图 2.13　设置监督人密码

(8) 选择“程序”|“运行”命令,在“运行”对话框中输入 regedit,打开注册表,在 HKEY_CURRENT_USER\Software\Microsoft\Internet Explorer\Main 分支下,修改 Start Page 等项的键值。

6. 实验报告与要求

根据上面介绍的各项实验要求,详细观察设置前后进行网络访问的变化,给出分析报告。

7. 实验分析与讨论

各项安全功能的增强,往往会带来网络访问的不便。在提高安全性的同时,为保证上网便利性,可以通过多种方法来实现,其中对访问空间进行分区是一种可行的途径。IE 提供的不同分区有四种:局域网、可信任站点、受限制站点、Internet 站点。可以将访问资源进行合理分类,并分别设置各分区的不同安全级别。

8. 注意事项

设置可信任站点时,对启用 SSL 加密链接的站点,需要添加 https 前缀。

2.2.2 网络监听与防范

1. 实验目的

掌握 Sniffer 捕获数据包的技术,了解一般局域网内监听手段,掌握如何防范攻击。

2. 实验原理

Sniffer 利用计算机的网络接口截获发往其他计算机的数据报文。它工作在网络的底层,把网络传输的全部数据记录下来,不仅可以使黑客和网络攻击者获取其他用户在网上发送的明文信息,也可以帮助网络管理员查找网络漏洞和检测网络性能,还可以分析网络的流量,以便找出所关心的网络中潜在的问题,在对网络犯罪进行侦察取证时获取有关犯罪行为的重要信息,成为打击网络犯罪的有力手段。Sniffer Pro 是一种常用的 Sniffer 工具。

3. 实验环境

三台互联的主机,IP 地址分别为 IP1、IP2、IP3,其中 Sniffer 程序安装在 IP 地址为 IP3 的主机上。

4. 实验内容

(1) 设置监听对象和内容;
(2) 获取监听内容并进行分析。

5. 实验步骤

(1) 打开 Sniffer Pro 程序,进入主界面,如图 2.14 所示。
(2) 选择 File|Select Settings 菜单,在弹出的对话框中选择要进行监听的网络接口所对应的网卡,并单击“确定”按钮,如图 2.15 所示。

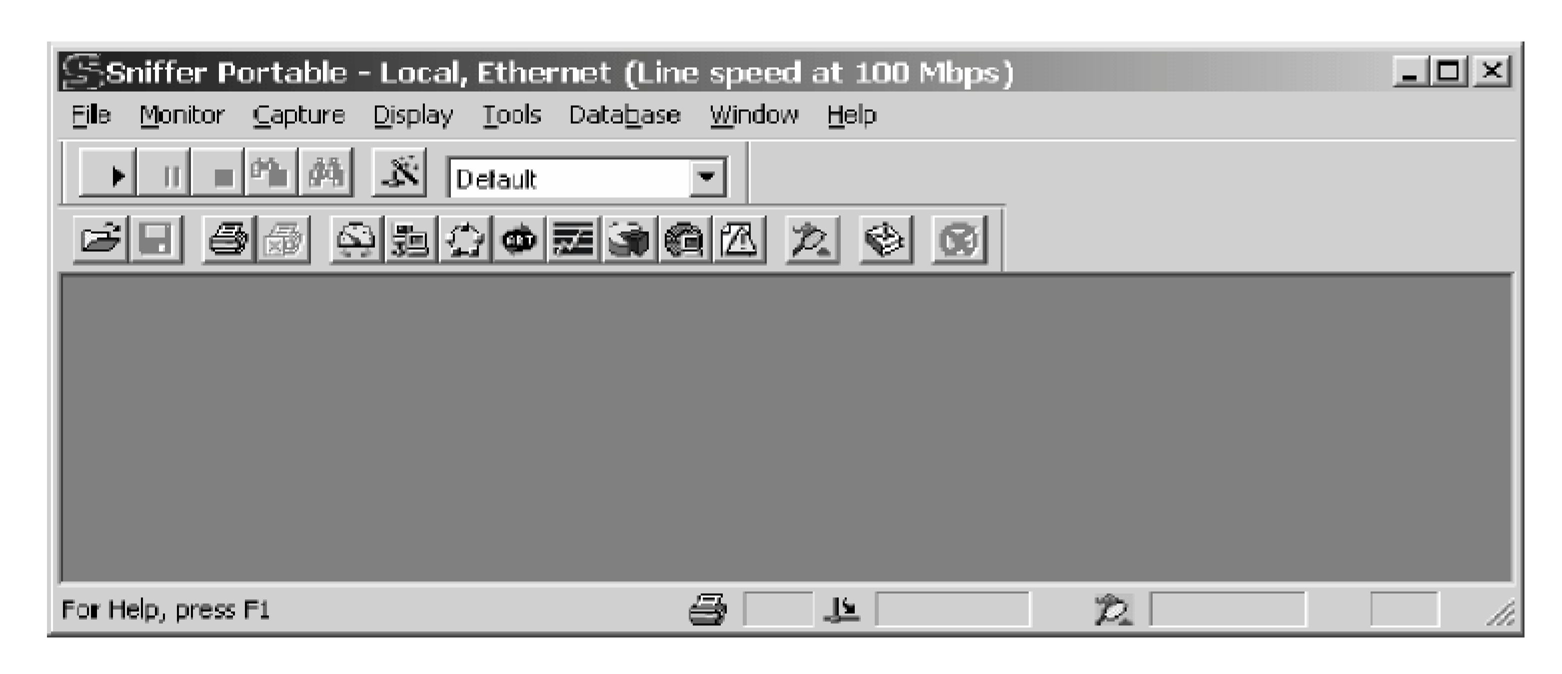


图 2.14　Sniffer Pro 主界面

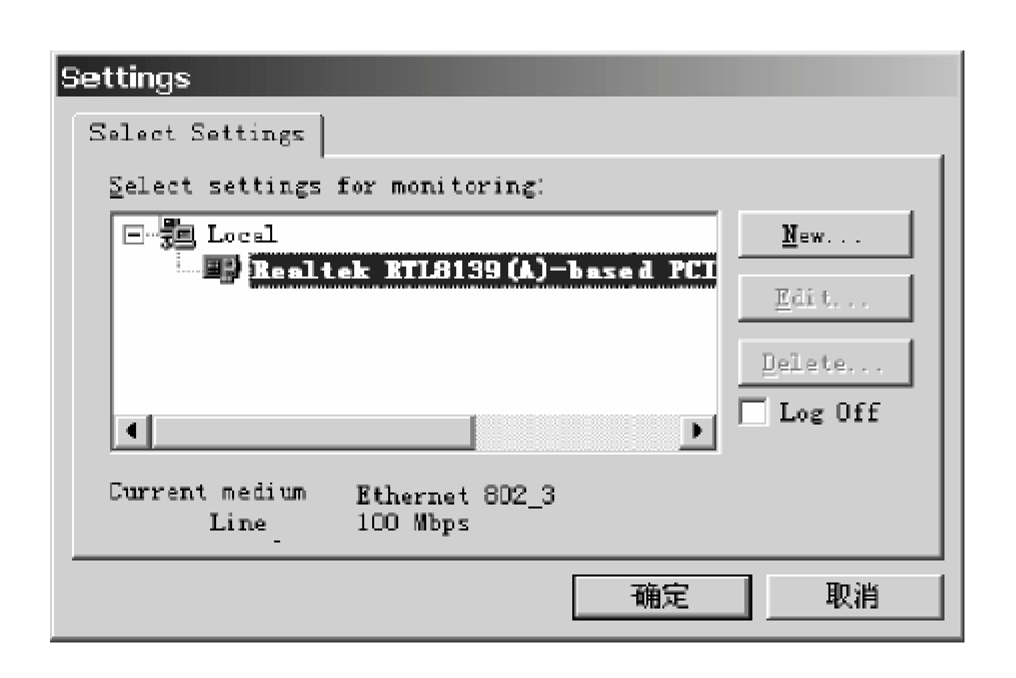


图 2.15　选择要进行监听的网络接口所对应的网卡

(3) 选择 Capture|Define Filter 菜单，在弹出的对话框中对默认抓包规则进行修改，如图 2.16 所示。

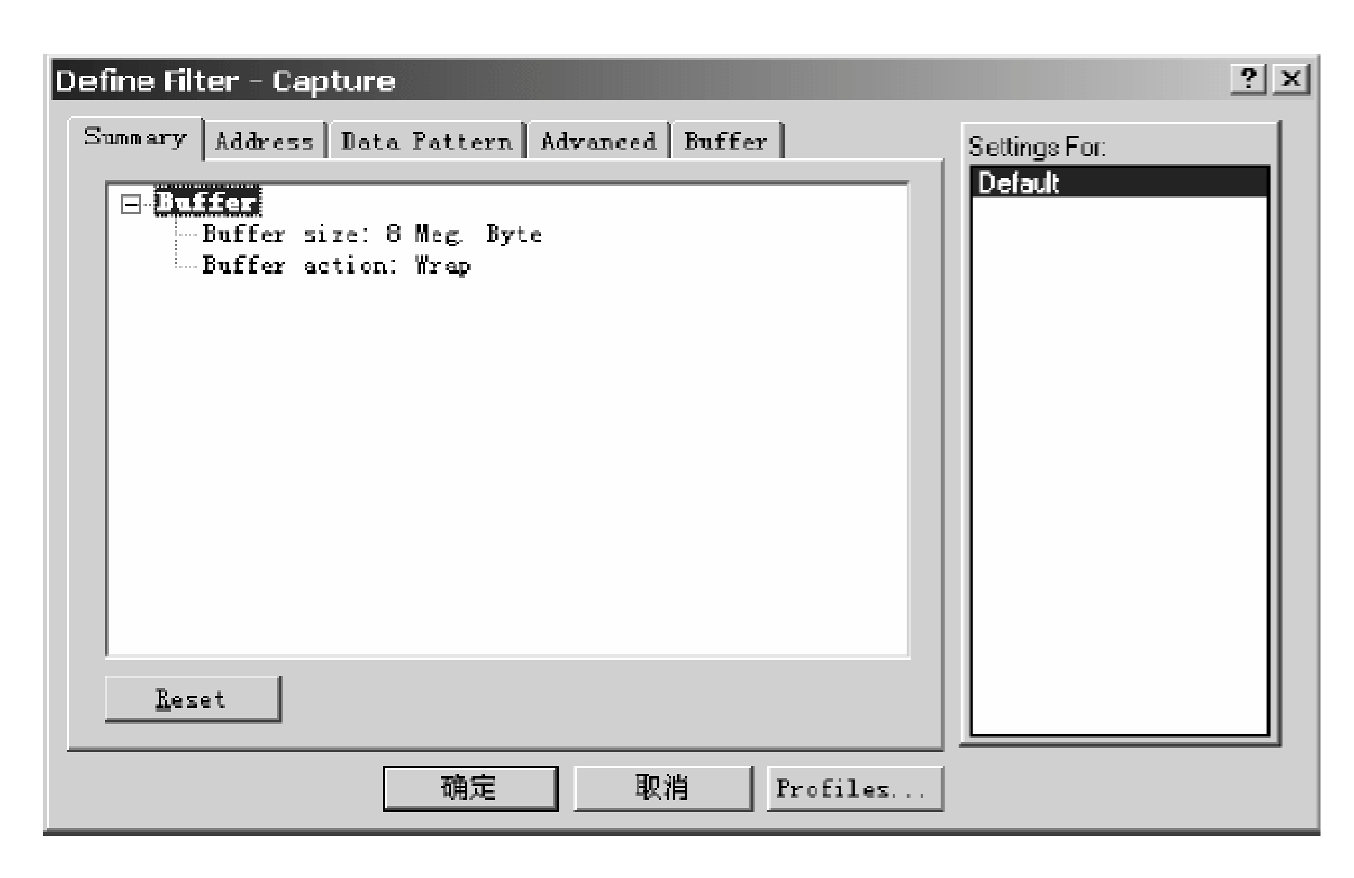


图 2.16　对默认抓包规则进行修改

(4) 打开 Address 选项卡，设置要监听的网络通信收发双方的地址，同时选中 IP 和 Include 模式，如图 2.17 所示。

(5) 打开 Advanced 选项卡，对要抓取的数据包的大小、类型及所使用的协议进行设置，本实验中选择 IP 及其下级选项 ICMP，其他设置不变，如图 2.18 所示。

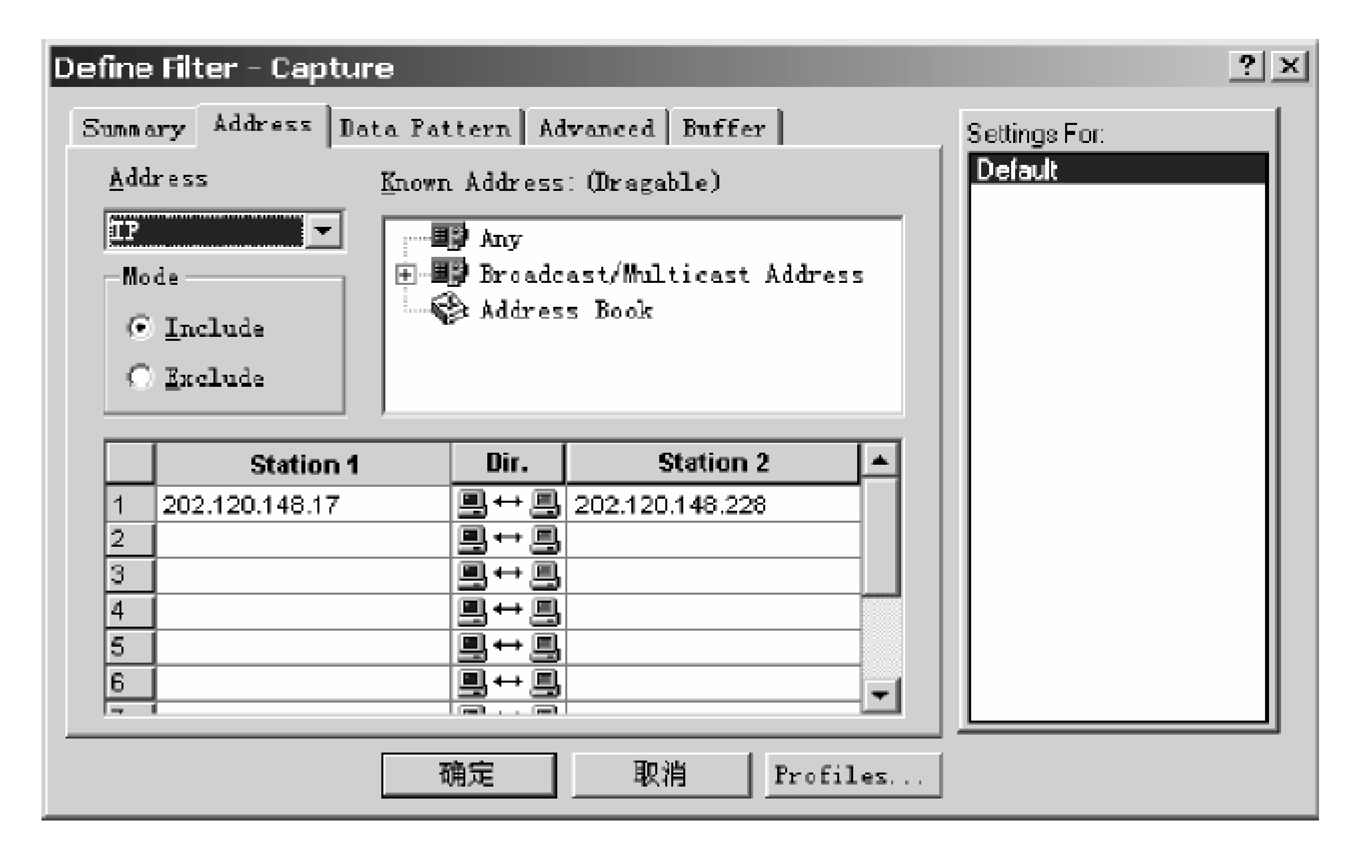


图 2.17 设置要监听的网络通信双方的地址

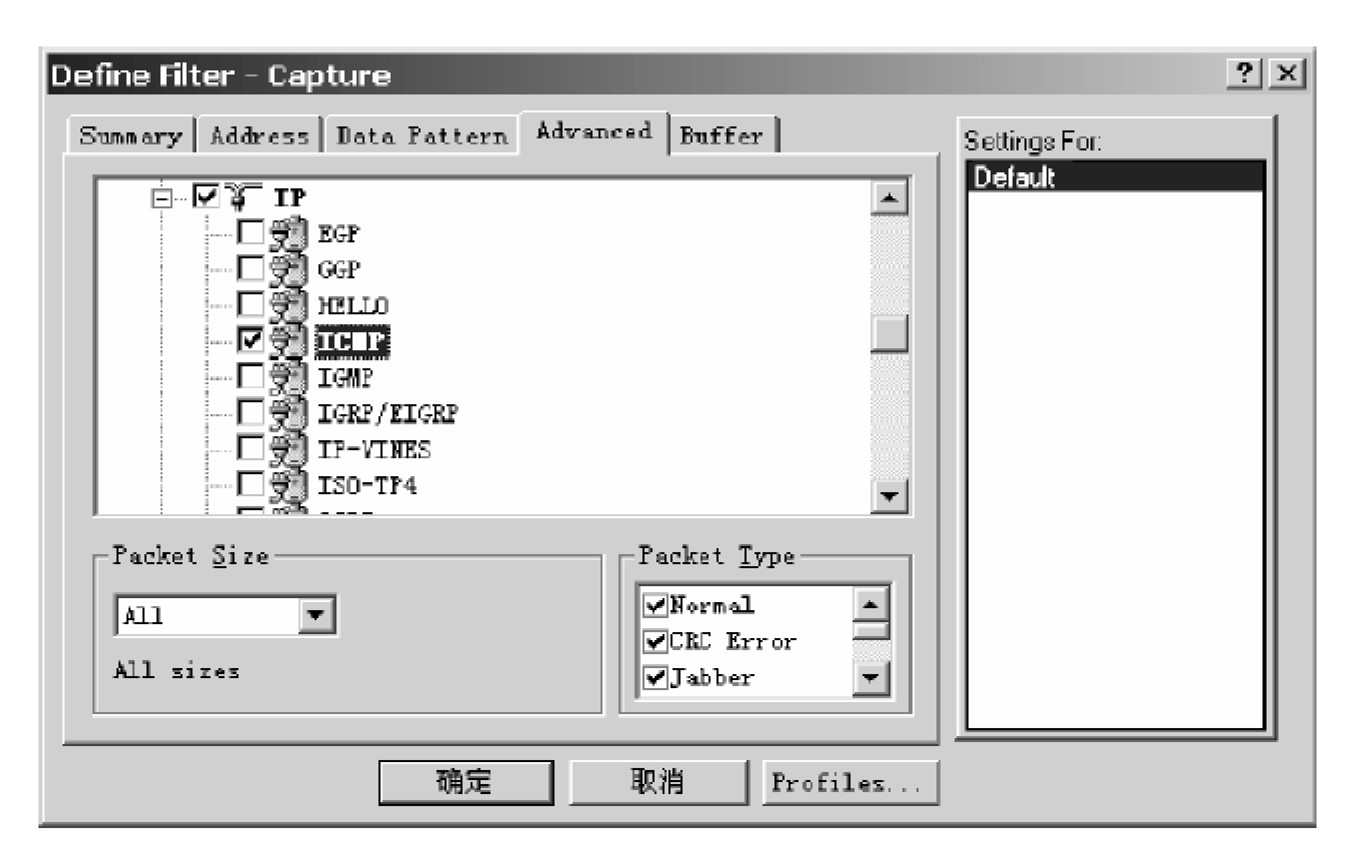


图 2.18 设置抓取数据包的类型及所使用的协议

（6）打开 Summary 选项卡，可看到修改后的过滤规则的完整描述，如图 2.19 所示。

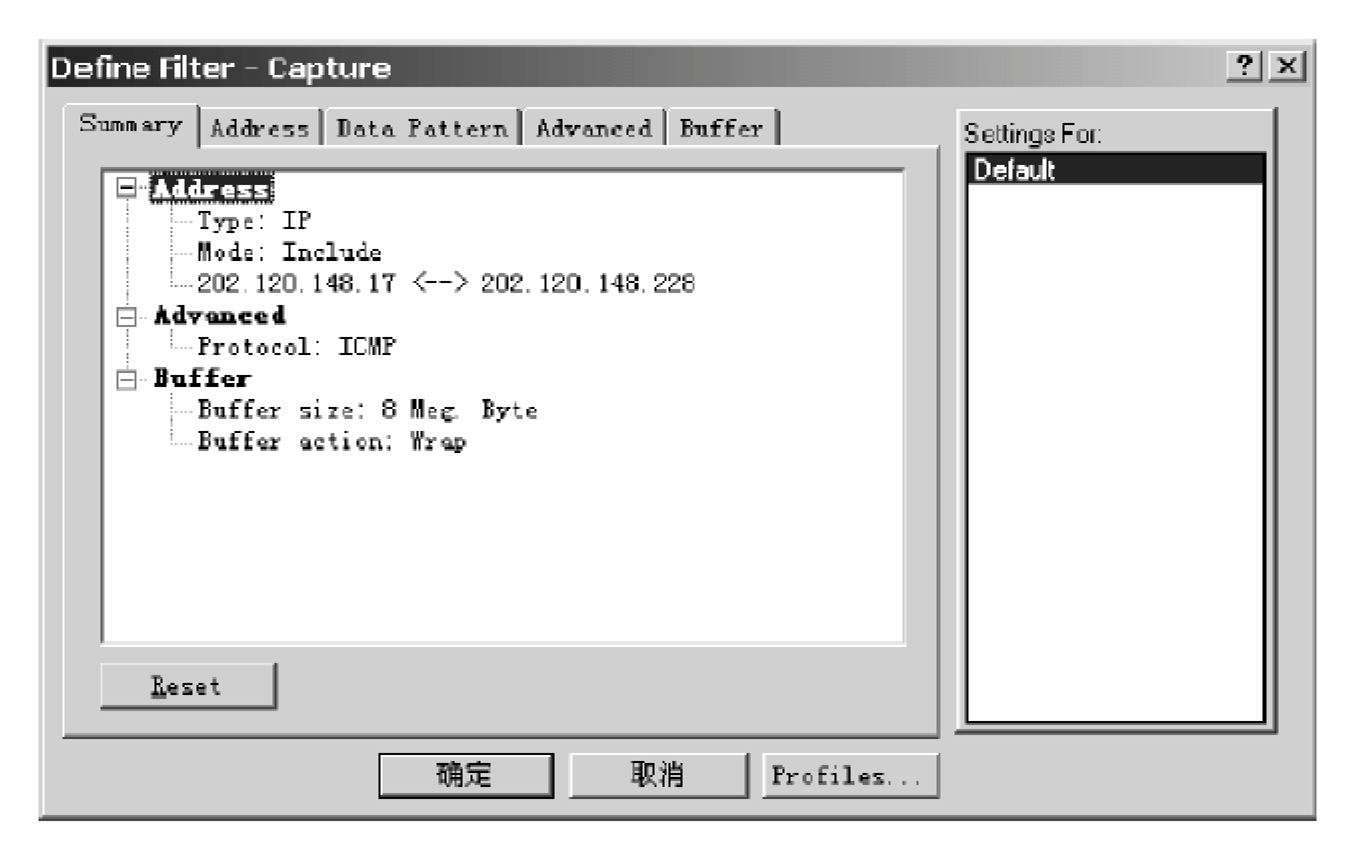


图 2.19 查看过滤规则

(7) 选择菜单栏中的 Capture|Start,开始捕获数据包。

(8) 令 IP1 主机 ping IP2 主机。

(9) 选择菜单栏中 Capture|Stop and Display,结束捕获数据包并显示结果。打开下面的 Decode 选项卡,得到捕获数据包的解码信息,如图 2.20 所示。

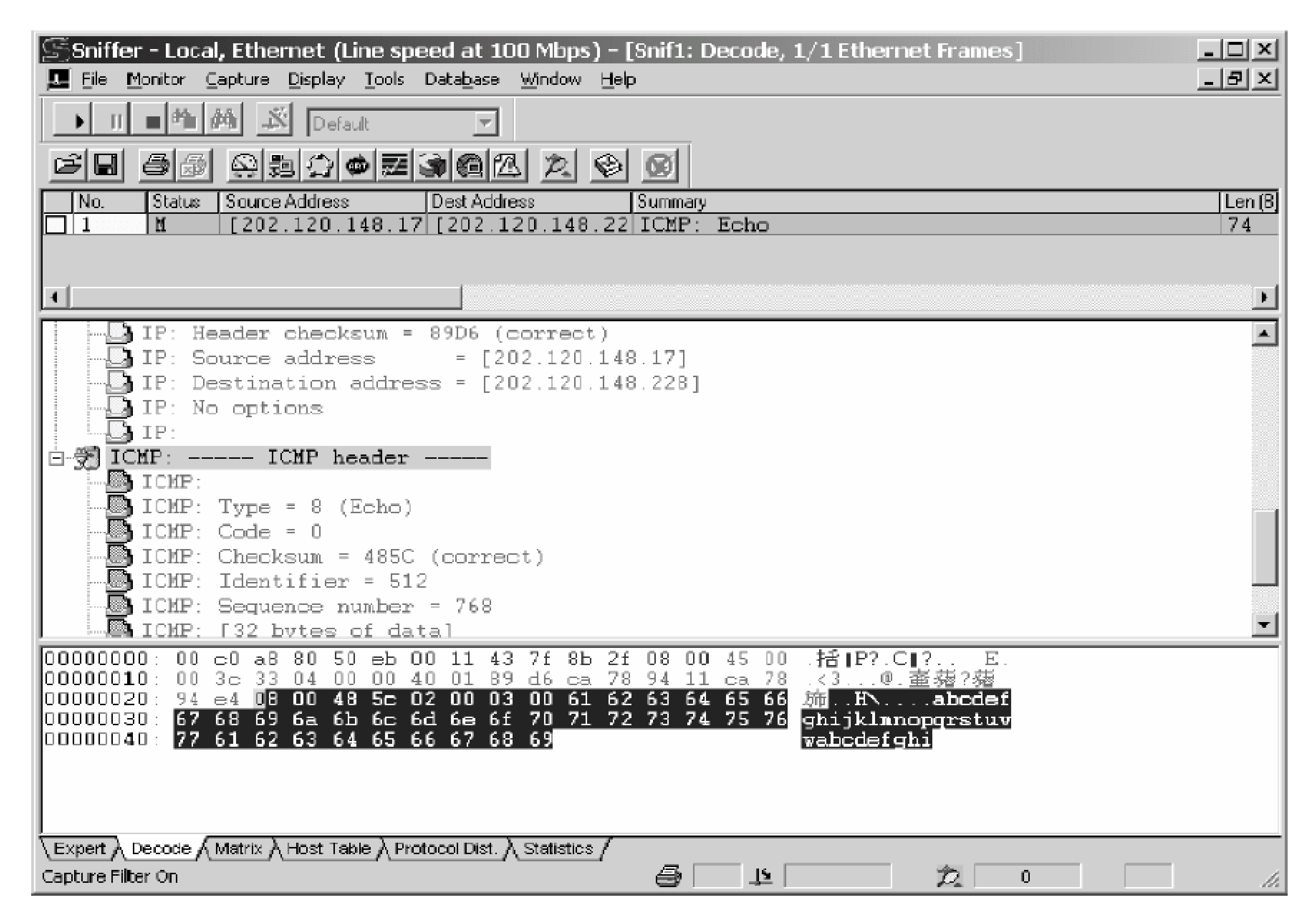


图 2.20　查看捕获数据包信息

6. 实验报告与要求

详细描述实验过程,仔细查看截获的数据,分析通过嗅探器能够获取哪些信息,撰写实验报告。

7. 实验分析与讨论

根据嗅探器工作原理,分析如何抵御嗅探器攻击。

8. 注意事项

(1) 实验时,可以由 3 个用户为一小组进行;

(2) 修改过滤规则中的协议,可以获得更多的数据包,但会对分析工作造成一定困难,因此,应根据需要进行设置;

(3) 在监听过程中,如果没有抓取数据包,则菜单栏中 Capture|Stop and Display 为灰色不可选项;

(4) 监听结果窗口中分为三个区域,从上到下分别为:截获的整个通信过程所有数据包的简要描述、选中数据包的详细结构和选中数据包的完整二进制表示。

2.2.3　木马攻击与防范

1. 实验目的

理解和掌握木马传播和运行的机制，掌握检查和删除木马的技巧，学会防御木马的相关知识，加深对木马的安全防范意识。

2. 实验原理

冰河木马是国内一款非常有名的木马程序，功能非常强大。该木马一般由两个文件组成：G_Client 和 G_Server，其中 G_Server 是木马的服务器端，是用来植入目标主机的程序，G_Client 是木马的客户端，即木马的控制端。当目标主机连接到因特网上时，木马程序就会统计被攻击者信息，报告主机 IP 地址以及预先设定的端口。攻击者在收到信息后，利用木马程序可以对目标计算机进行各种操作。

3. 实验环境

两台主机，一台安装 Windows 2000 Pro 或者 Windows XP 操作系统，另一台安装 Windows 2000 Server 操作系统。

4. 实验内容

(1) 安装冰河木马程序的客户端；
(2) 攻击目标主机，安装冰河木马程序的服务器端；
(3) 运行客户端程序对目标计算机进行控制；
(4) 删除冰河木马。

5. 实验步骤

(1) 运行冰河木马程序，选择菜单"设置"|"配置服务程序"命令，打开的窗口如图 2.21 所示。



图 2.21　冰河木马主界面

（2）设置待配置文件为 C:\WINDOWS\system32\TaiGu\glacier\G_SERVER.EXE，设置访问口令为 111111，其他为默认值，单击“确定”按钮，生成木马的服务端程序 G_SERVER.EXE，如图 2.22 所示。



图 2.22　进行服务器端配置

（3）关闭目标主机防火墙和杀毒软件的自动防护功能，运行木马服务器端程序 G_SERVER.EXE。

（4）打开木马客户程序，单击“添加计算机”按钮，在“显示名称”中输入显示在主界面的名称，“主机地址”中输入服务端主机 IP 地址，“访问口令”中输入 111111，“监听端口”中输入冰河木马的默认监听端口 7626，如图 2.23 所示。

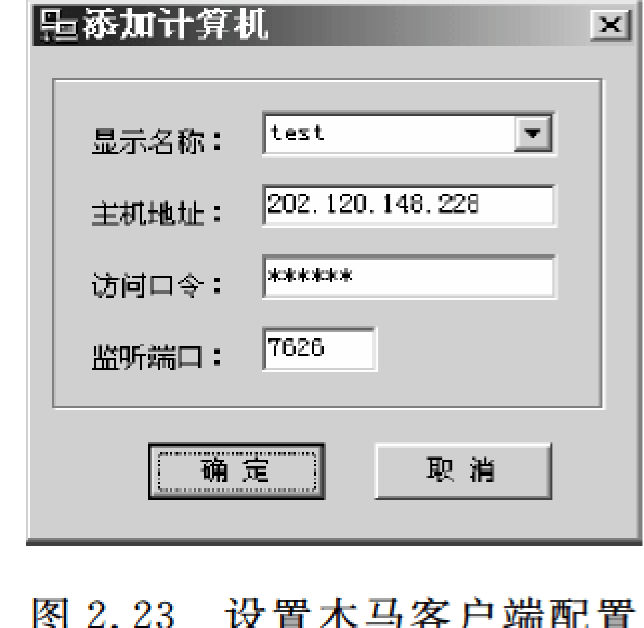


图 2.23　设置木马客户端配置

（5）在主界面窗口可以看到添加了主机，如图 2.24 所示。

（6）打开主界面中“命令控制台”选项卡，单击“口令类命令”，查看目标主机相关信息，如图 2.25 所示。

图 2.24　查看所添加主机信息



图 2.25　查看目标主机相关信息

(7) 打开“控制类命令”，了解木马可实现的操作，如图 2.26 所示。



图 2.26　查看控制类命令

(8) 了解其他控制命令，如图 2.27 和图 2.28 所示。



图 2.27　查看网络类命令和文件类命令



图 2.28　查看设置类命令

（9）打开注册表，手动卸载冰河木马程序。

① 在 HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Run 中，删除默认键值 C:\WINDOWS\system32\KERNEL32.EXE，如图 2.29 所示。



图 2.29　修改注册表启动程序

② 将注册表中 HKEY_CLASSES_ROOT\txtfile\shell\open\command 下的默认值改为 C:\WINDOWS\notepad.exe %1，恢复被木马程序修改的 txt 文件关联程序，如图 2.30 所示。

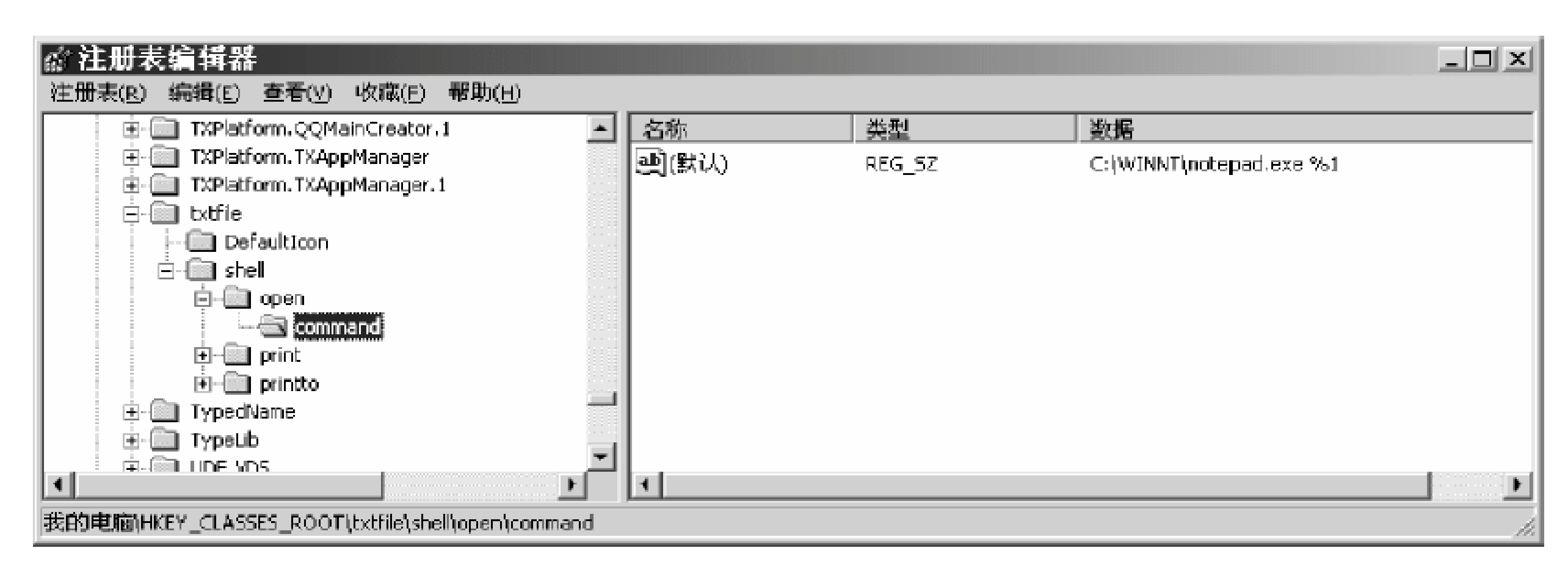


图 2.30　修改注册表文件关联程序

③ 进入 C:\WINDOWS\system32 目录，找到并删除冰河木马的两个可执行文件 KERNEL32.EXE 和 SYSEXPLR.EXE，如图 2.31 所示。

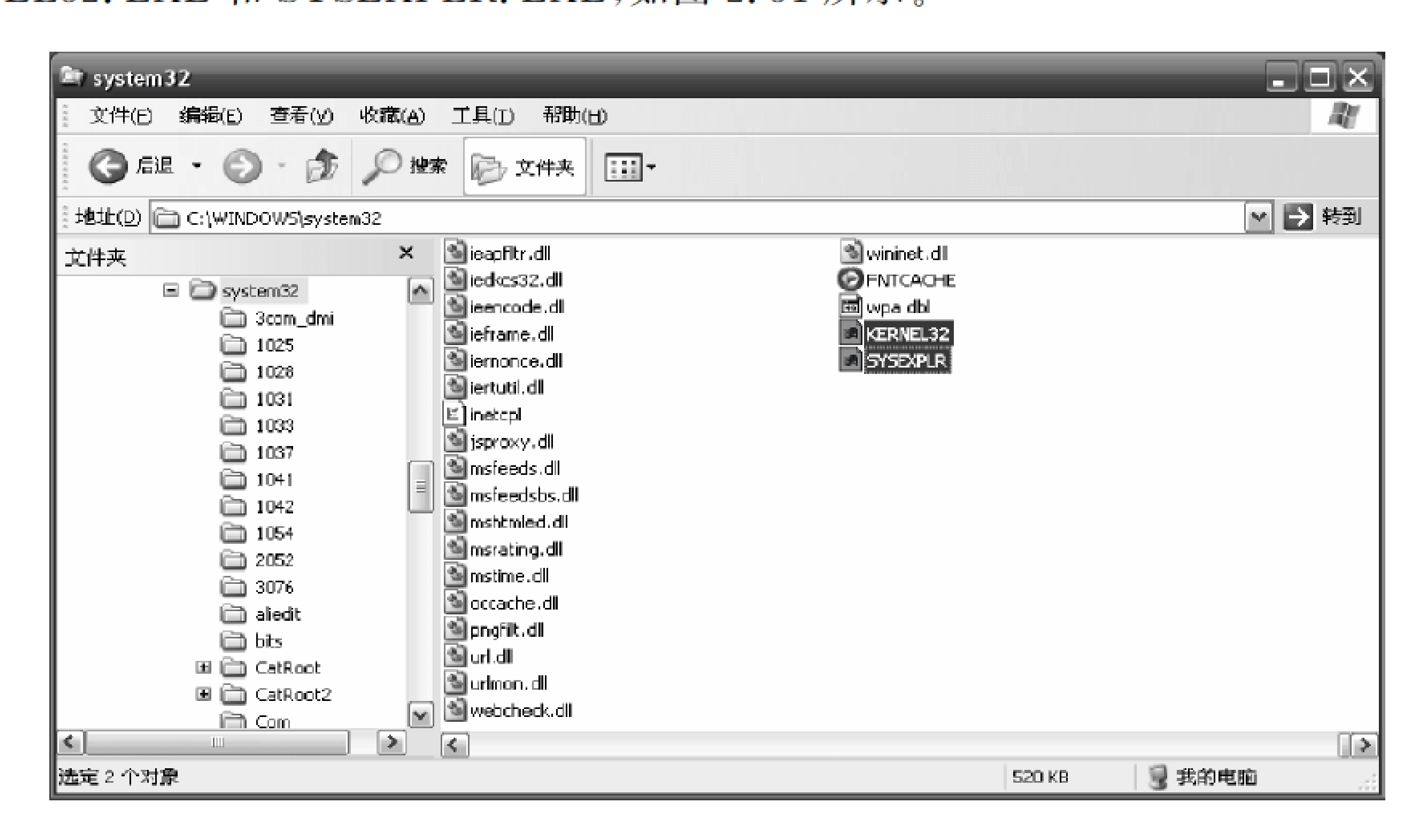


图 2.31　删除木马文件

6. 实验报告与要求

详细描述实验过程，分析木马程序会对主机造成哪些危害，撰写实验报告。

7. 实验分析与讨论

了解还有哪些常见的木马程序，它们的加载、使用和攻击方式有何不同，并了解和使用常用的木马查杀工具，思考如何防范木马攻击。

8. 注意事项

（1）实验前需要关闭服务端主机杀毒软件的自动防护功能和防火墙，否则程序会被当作病毒而强行终止；

（2）删除冰河木马程序除了采用手工方式外，也可以在客户端自动卸载或使用杀毒软件进行查杀。

2.2.4　DDoS 攻击与防范

1. 实验目的

通过使用拒绝服务（DoS）工具和分布式拒绝服务（DDoS）攻击工具对目标主机进行攻击，理解 DoS/DDoS 攻击的原理及实施过程，了解 IPv4 的固有缺陷。

2. 实验原理

SYN Flood 是目前较常见的 DoS/DDoS 的方式之一，该方式利用 TCP 协议缺陷，发送

大量伪造的TCP连接请求，使得被攻击方资源耗尽，系统无法运行或者服务可用性大大降低。

3. 实验环境

两台或多台相连的运行Windows 2000操作系统的计算机。

4. 实验内容

采用SYN Flood工具进行拒绝服务攻击。

5. 实验步骤

(1) 打开目标主机的防护软件的实时监控功能。

(2) 打开命令行窗口，进入syn的对应目录，运行syn.exe，根据提示输入目标IP和端口(一般为139)，开始攻击，如图2.32所示。

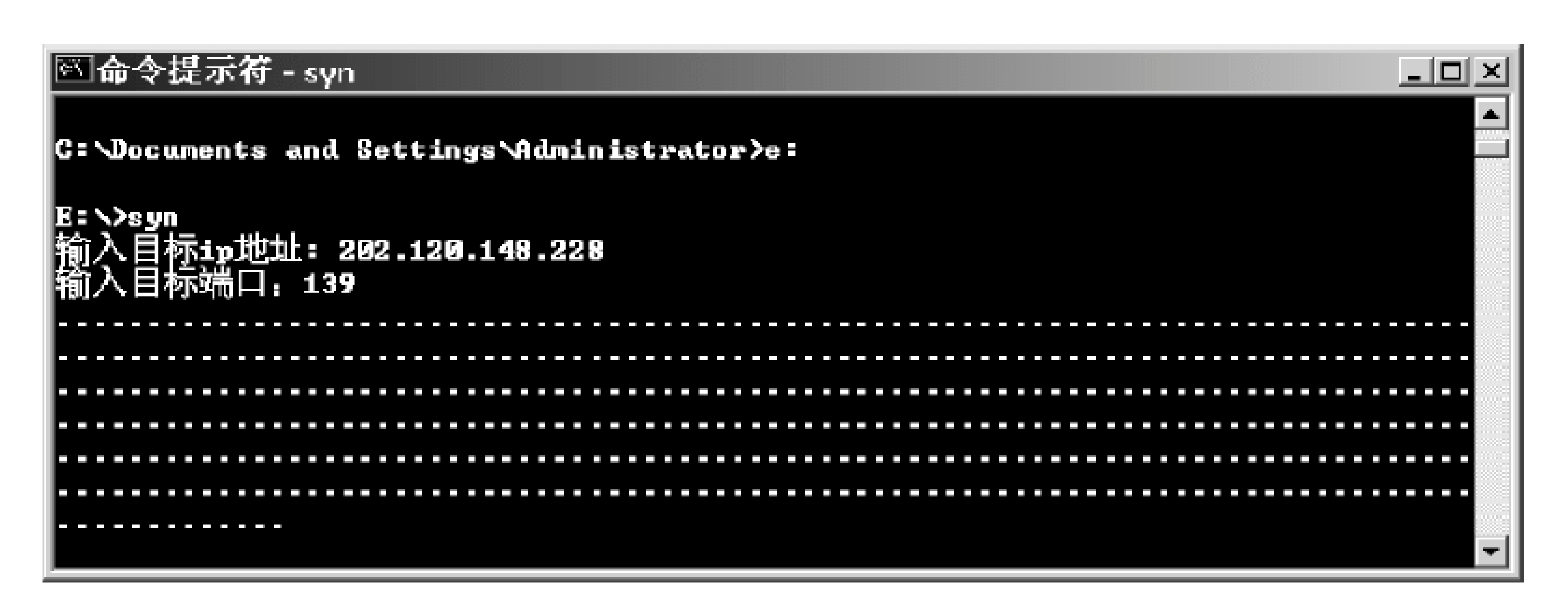


图2.32　运行拒绝服务攻击

(3) 查看目标主机防护软件阻止攻击情况，如图2.33所示。



图2.33　查看目标主机防护软件对攻击的截获

6. 实验报告与要求

根据上面介绍的实验要求，两人一组考察攻击前后目标主机的变化，给出分析报告。

7. 实验分析与讨论

在没有安装任何补丁的两台主机间进行拒绝服务攻击，观察攻击过程。同时根据拒绝服务攻击的原理，制订出防范该攻击的措施。

8. 注意事项

（1）本实验中由于目标主机已安装相关的系统补丁和防护软件，SYS Flood 没有成功，在屏幕上显示无数据包成功发送，如果攻击成功，则屏幕上会显示具体的发送数据包信息。

（2）目标主机虽然成功阻止 SYS Flood 攻击，但系统性能仍然会受到一定影响，实验中可以观察到。

2.2.5 网络扫描技术

1. 实验目的

了解扫描技术的工作原理，掌握常用扫描工具的基本用法。

2. 实验原理

X-Scan 是由国内著名的网络安全站点“安全焦点”开发的一款运行在 Windows 平台下、免费的扫描工具。X-Scan 采用多线程方式对指定的 IP 地址段（或单主机）进行安全漏洞检查，支持插件功能，提供了图形界面和命令行两种操作方式。扫描的内容包括远程操作系统类型及版本、标注端口状态及端口 Banner 信息、各种弱口令漏洞、RPC 漏洞、CGI 漏洞、后门、网络设备漏洞以及拒绝服务漏洞等。X-Scan 把扫描报告和安全焦点网站相链接，对扫描到的每个漏洞进行“风险等级”评估，并提供漏洞描述、利用程序及解决方案。

3. 实验环境

两台安装 Windows 2000/XP 的主机，其中一台安装 X-Scan v3.0 绿色免安装版软件。

4. 实验内容

（1）设置 X-Scan 软件；

（2）扫描本机漏洞；

（3）对网络目标主机进行探测。

5. 实验步骤

（1）运行 X-Scan 主程序，浏览主界面中对软件的介绍，如图 2.34 所示。

（2）选择“扫描模块”图标，对将要扫描的内容进行设置，如图 2.35 所示。

（3）选择“扫描参数”图标，打开“扫描参数”对话框，单击其中的“基本设置”选项卡，设置检测主机的 IP 地址为 127.0.0.1，对本机进行扫描，如图 2.36 所示。

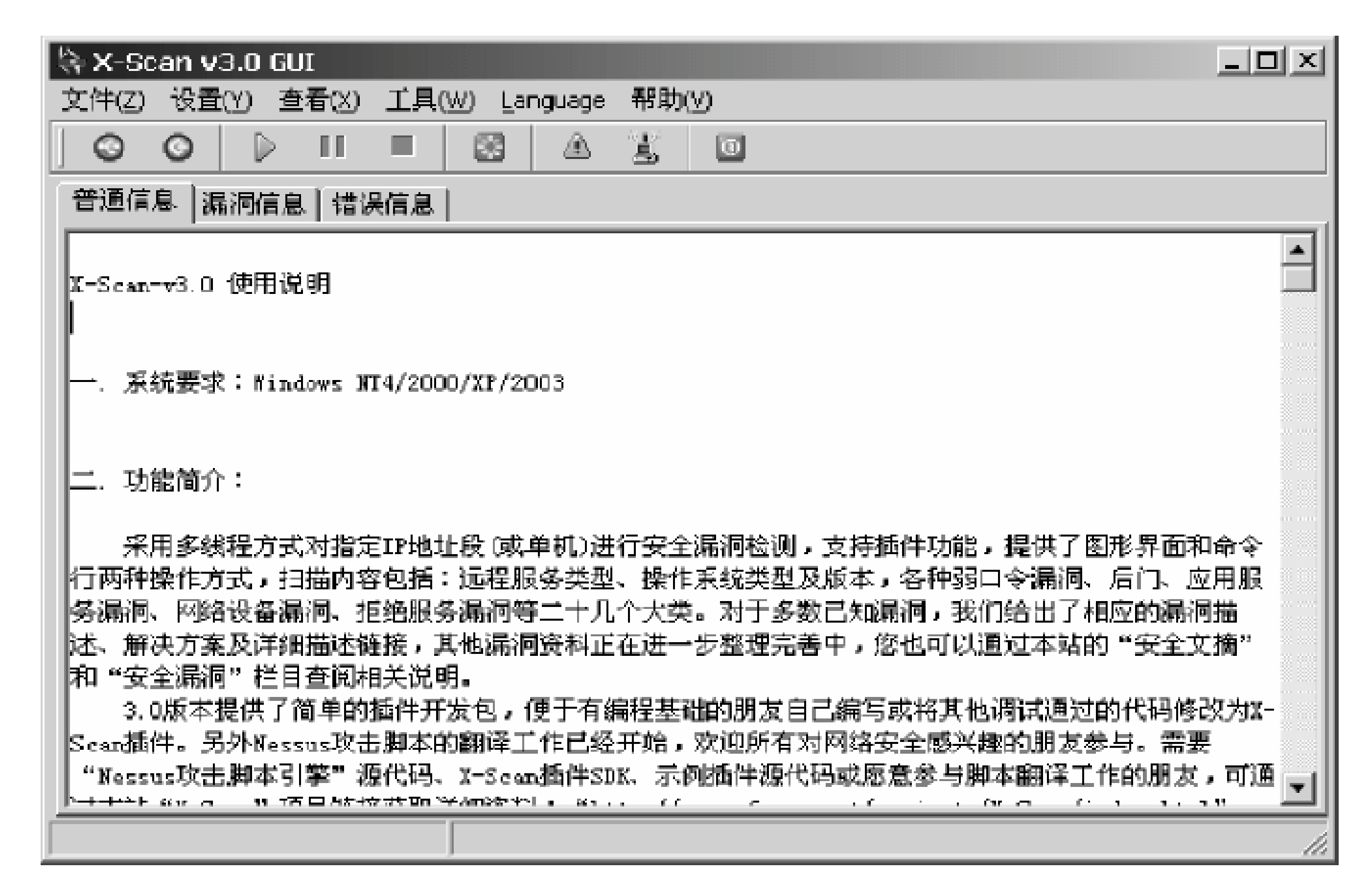


图 2.34　X-Scan 主界面



图 2.35　配置扫描模块

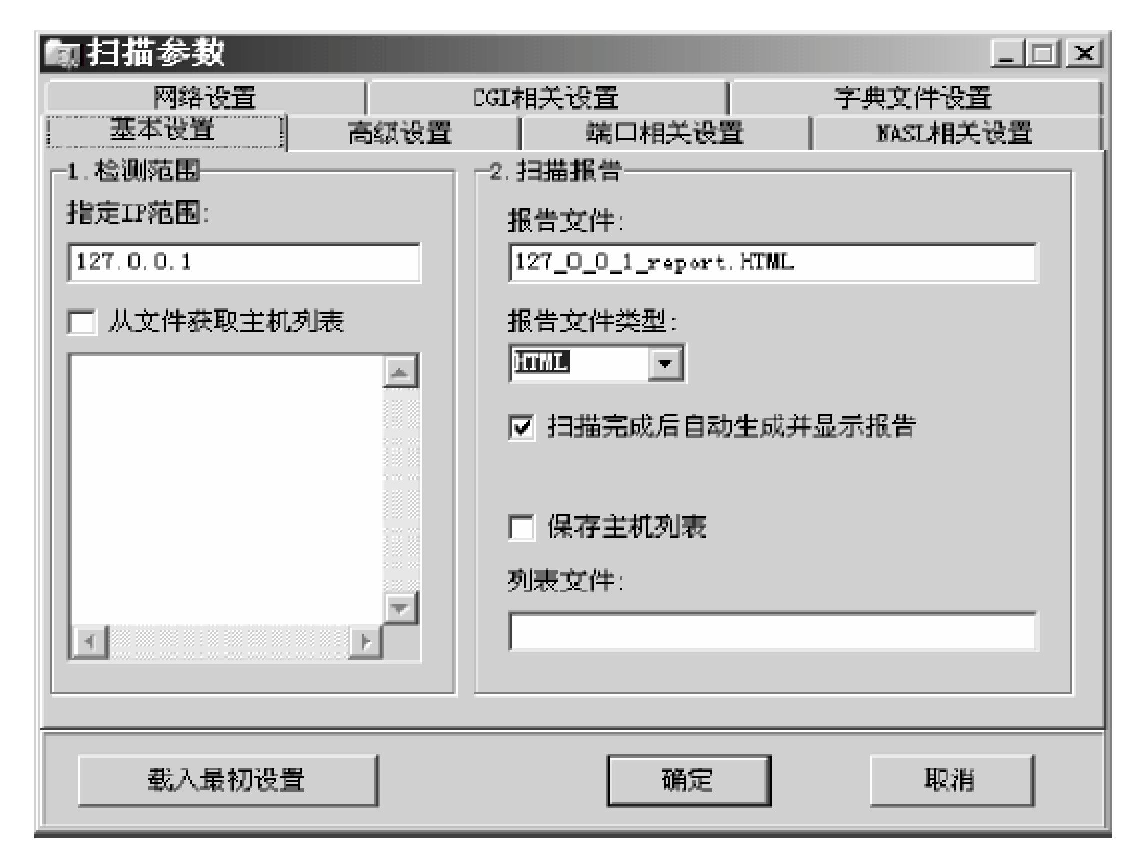


图 2.36　设置对本机扫描参数

(4) 打开"端口相关设置"选项卡，设置需要扫描的端口，如图 2.37 所示。

(5) 选择主界面菜单"工具"|"物理地址查询"命令，打开"物理地址查询"选项卡，可以对目标主机进行相关查询，如图 2.38 所示。

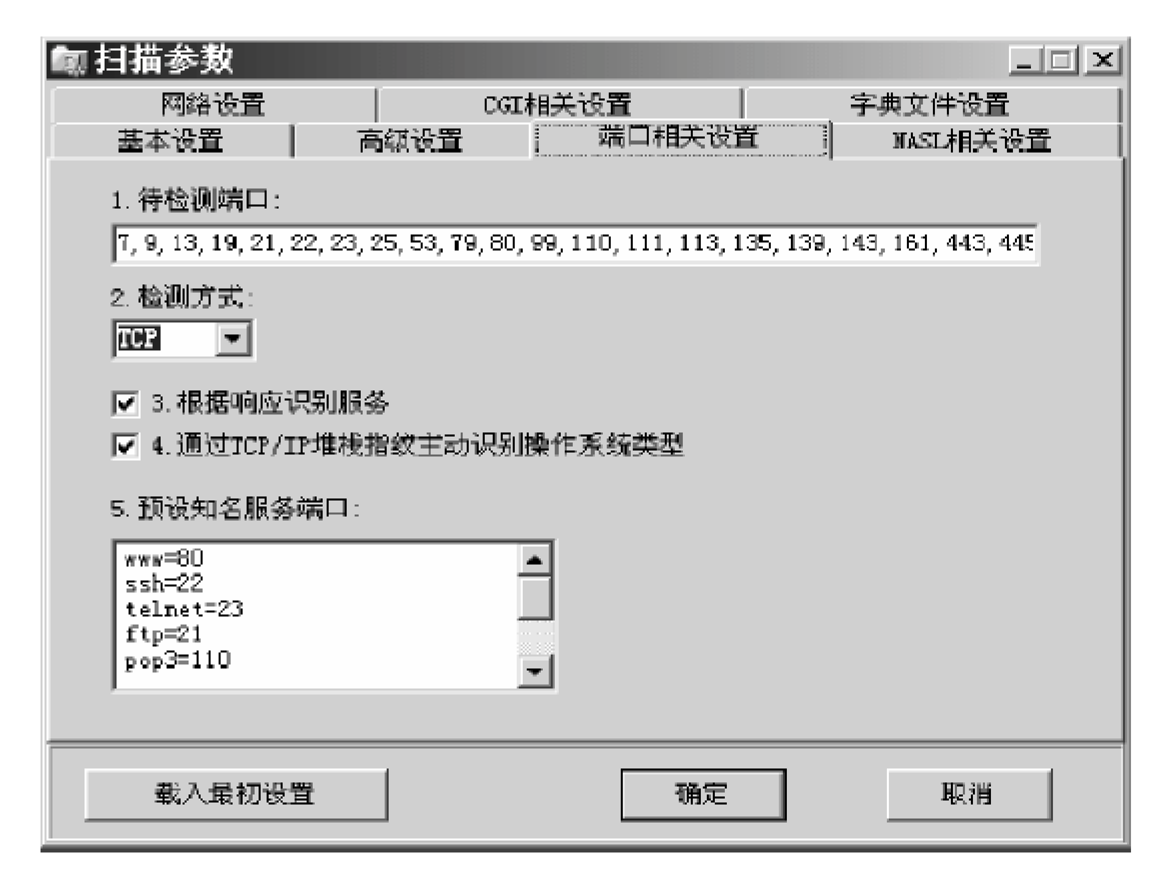


图 2.37　设置检测端口



图 2.38　查询目标主机信息

(6) 选择“开始扫描”图标，开始对本机进行扫描，如图 2.39 所示。

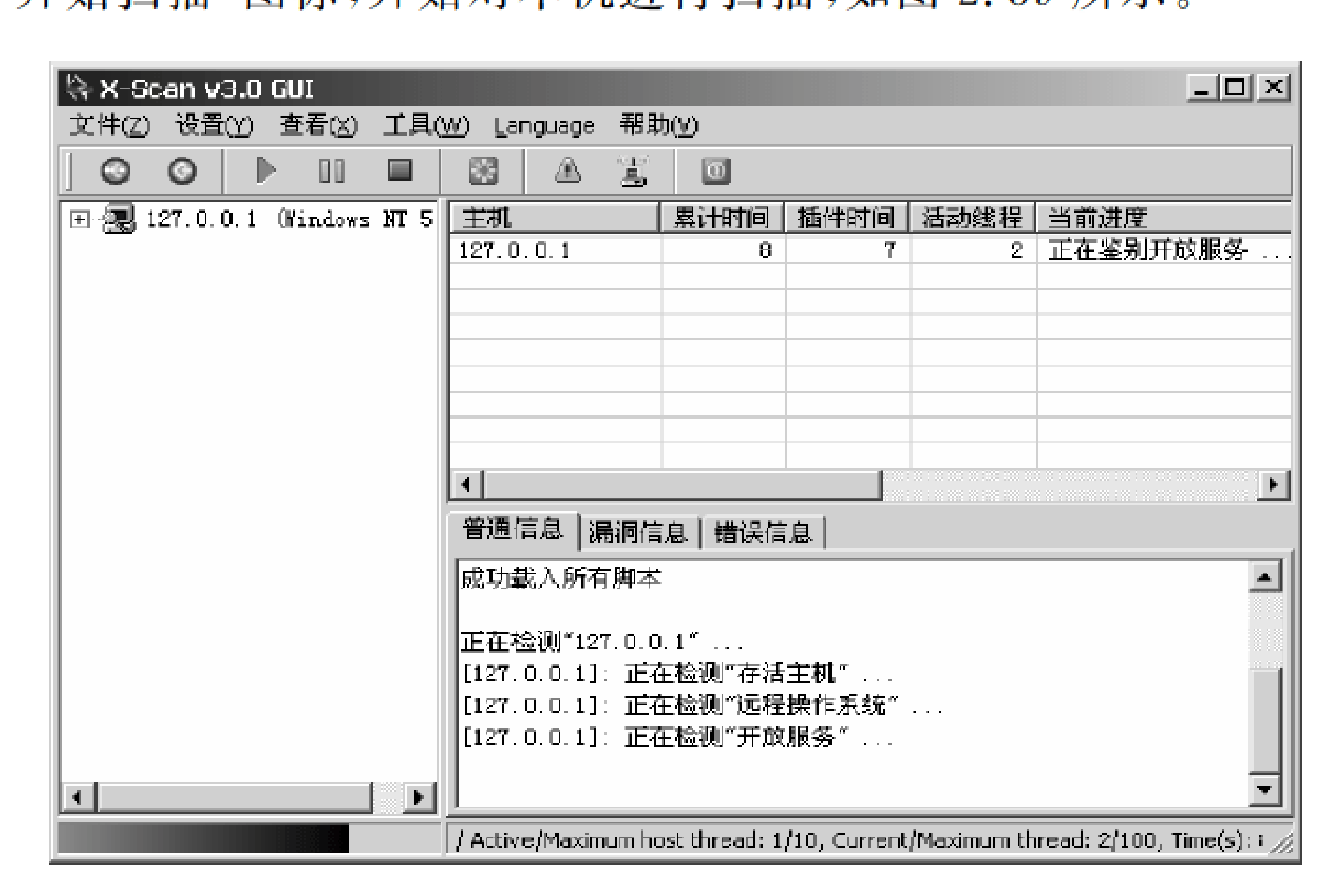


图 2.39　对本机进行扫描

（7）扫描结束，单击“漏洞信息”查看本机的漏洞信息，如图 2.40 所示。

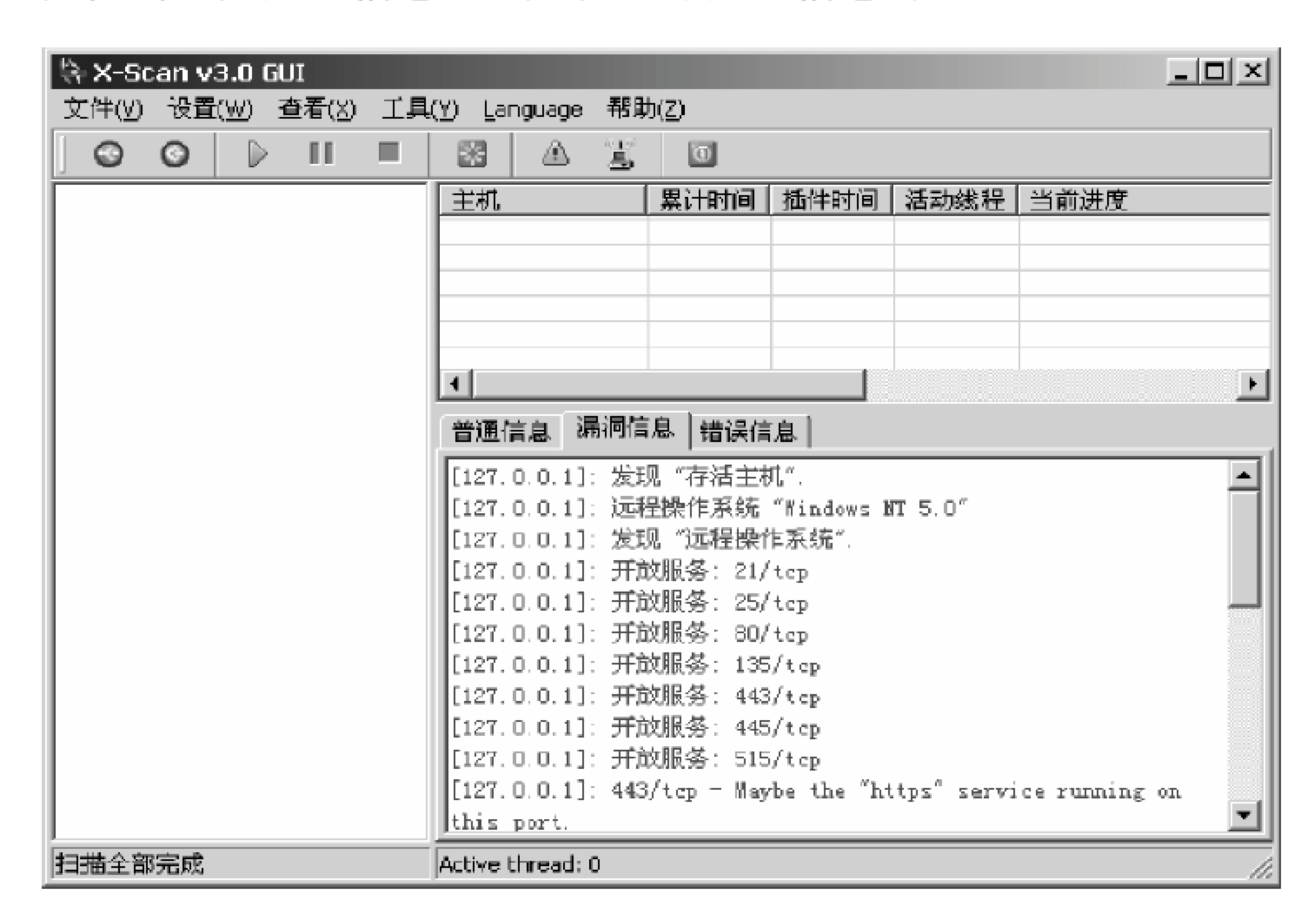


图 2.40　查看本机扫描的漏洞信息

（8）单击“扫描报告”，查看扫描结果，如图 2.41 所示。



图 2.41　查看本机扫描结果报告

(9) 选择"扫描参数"图标,打开设置对话框,选择其中的"基本设置"选项卡,设置检测主机的 IP 地址为 202.120.148.228,如图 2.42 所示。

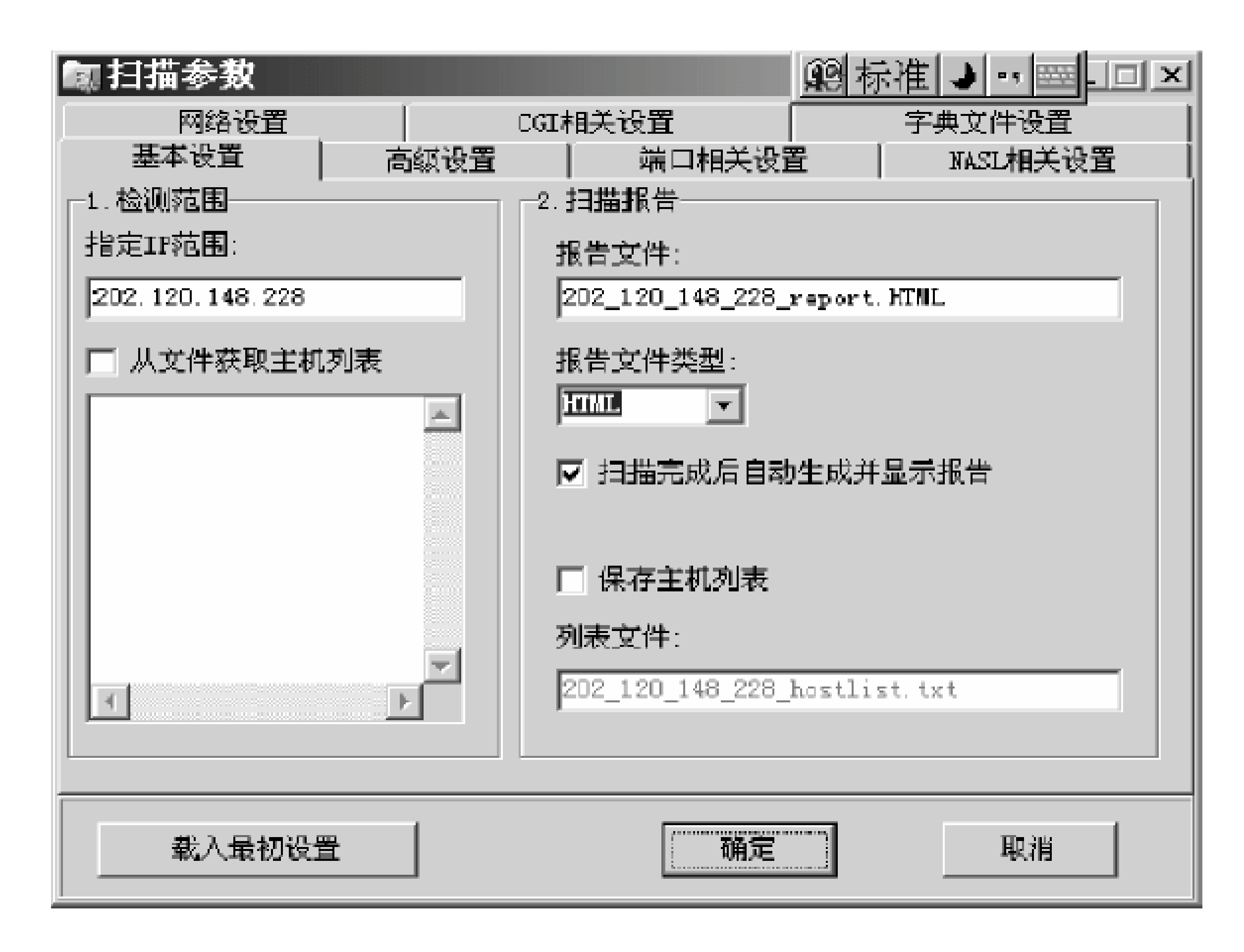


图 2.42　配置目标主机扫描信息

(10) 单击"开始扫描"图标,对网络目标主机进行扫描,如图 2.43 所示。

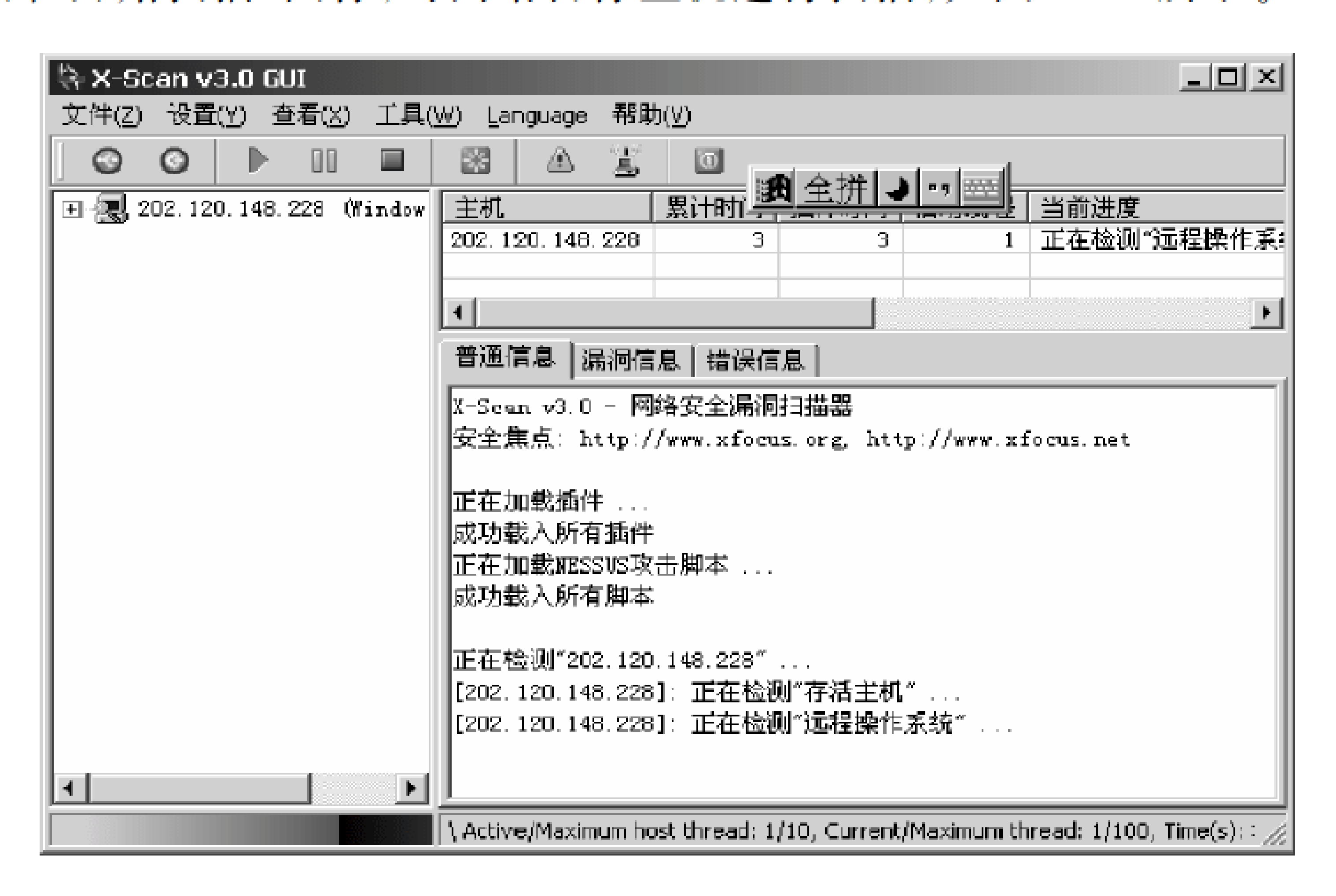


图 2.43　对目标主机进行扫描

(11) 扫描结束,单击"漏洞信息"查看本机的漏洞信息,如图 2.44 所示。

(12) 单击"扫描报告",查看扫描结果,如图 2.45 所示。

6. 实验报告与要求

根据上面介绍的各项实验要求,详细观察记录 X-Scan 的使用方法,分析对本机和目标主机的扫描结果,给出实验报告。

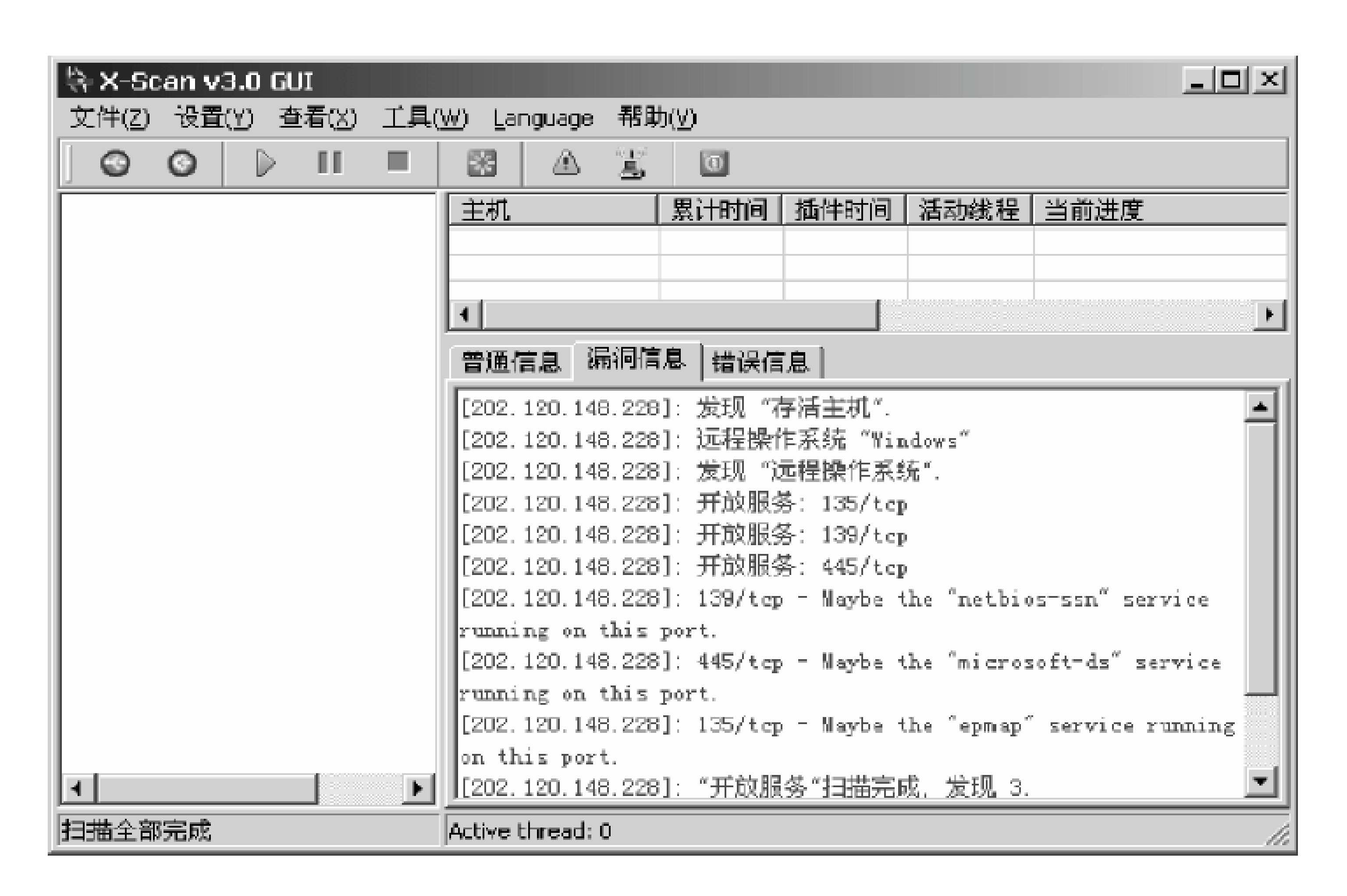


图 2.44　查看目标主机扫描漏洞信息



图 2.45　查看目标主机扫描结果报告

7. 实验分析与讨论

作为网络管理员，应该如何利用网络扫描技术对所维护的系统进行审计。为了对抗网络扫描，可以采取哪些基本措施。对于普通用户，为保障网络安全可以采用的设置和工具有哪些。

8. 注意事项

本实验中对目标主机进行扫描时,应关闭目标主机上的防护软件,否则扫描可能会因为被拦截而失败。

2.2.6 防火墙的使用

1. 实验目的

通过实验进一步加深对防火墙有关知识的理解,并掌握个人防火墙的安装和使用,灵活运用防火墙的配置,保证系统的安全。

2. 实验原理

天网防火墙个人版是由天网安全实验室研发制作给个人计算机使用的网络安全工具。它根据系统管理者设定的安全规则把守网络,提供强大的访问控制、应用选通、信息过滤等功能。它可以帮助抵挡网络入侵和攻击,防止信息泄露,保障用户机器的网络安全。天网防火墙把网络分为本地网和互联网,可以针对来自不同网络的信息,设置不同的安全方案,适合于任何方式连接上网的个人用户。

3. 实验环境

运行 Windows 2000 的主机一台。

4. 实验内容

(1) 安装天网个人防火墙;
(2) 配置并使用天网个人防火墙。

5. 实验步骤

(1) 单击天网个人防火墙安装程序,按照提示进行安装,如图 2.46 所示。

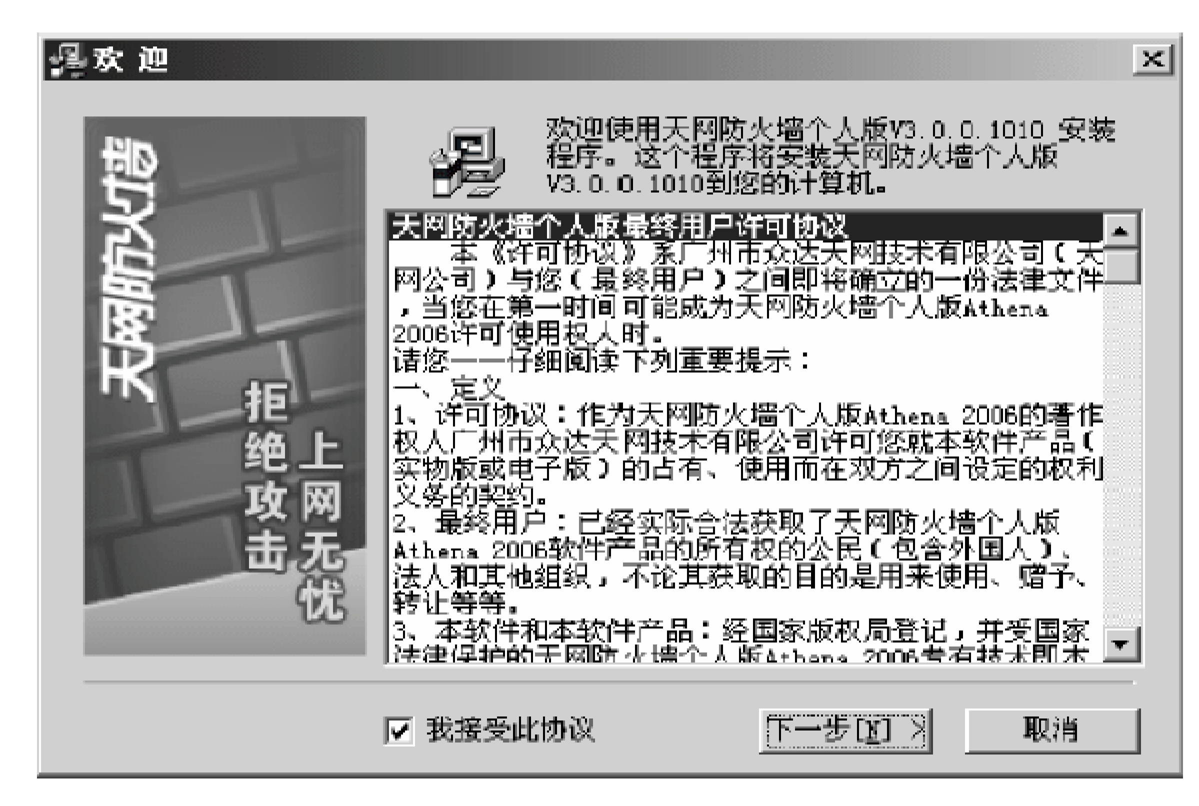


图 2.46 安装天网个人防火墙

(2) 完成安装后,按照提示对系统进行初步设置,如图 2.47 和图 2.48 所示。



图 2.47 设置系统安全级别

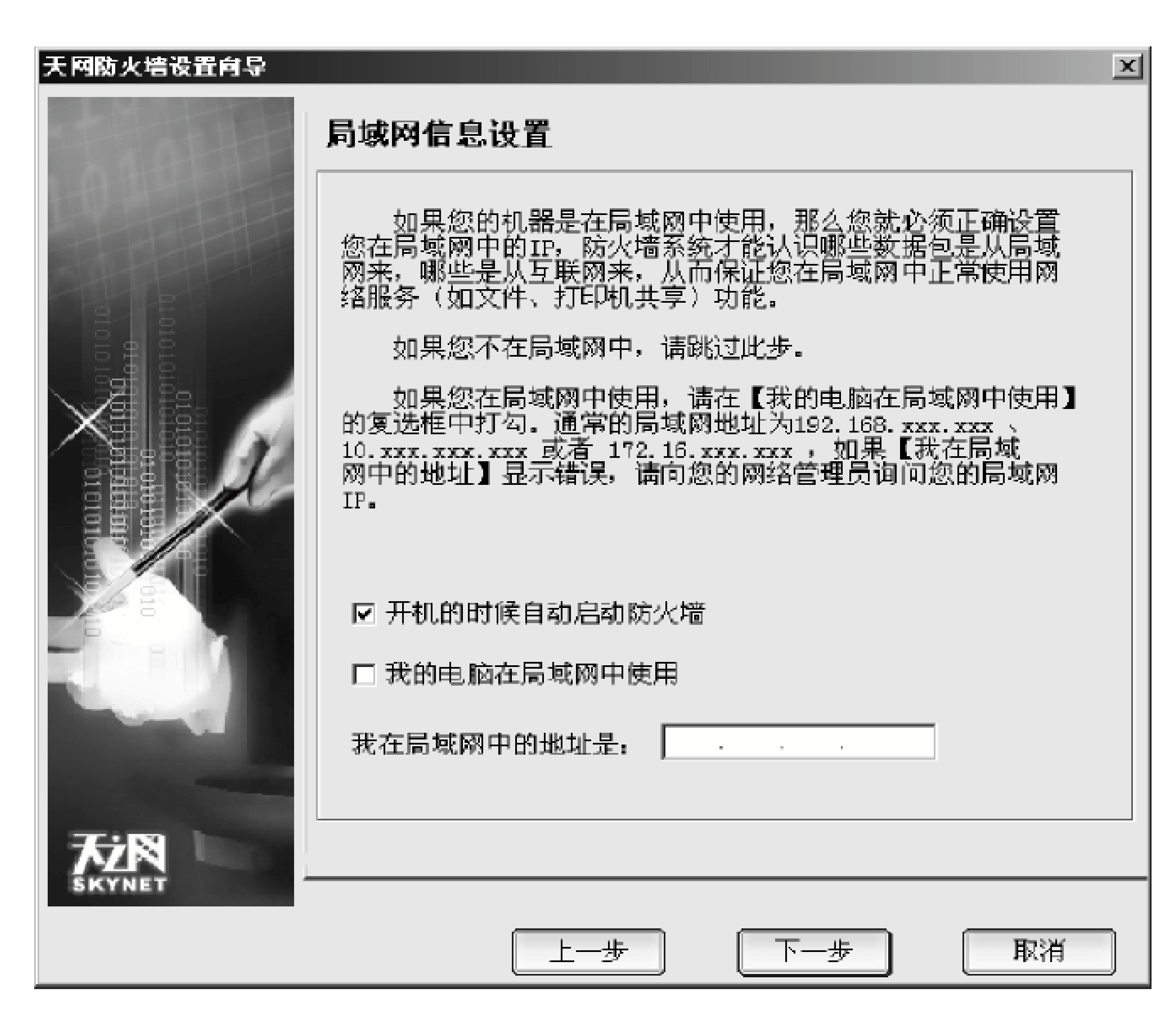


图 2.48 设置防火墙开机启动方式

(3) 重启系统运行防火墙程序。

(4) 在主界面中重新对系统的安全级别进行设置,如图 2.49 所示。

(5) 单击"自定义"图标,选中窗口中某项 IP 规则打开设置对话框,可以对该规则进行详细设置,如图 2.50 和图 2.51 所示。



图 2.49　设置系统安全级别



图 2.50　自定义 IP 规则

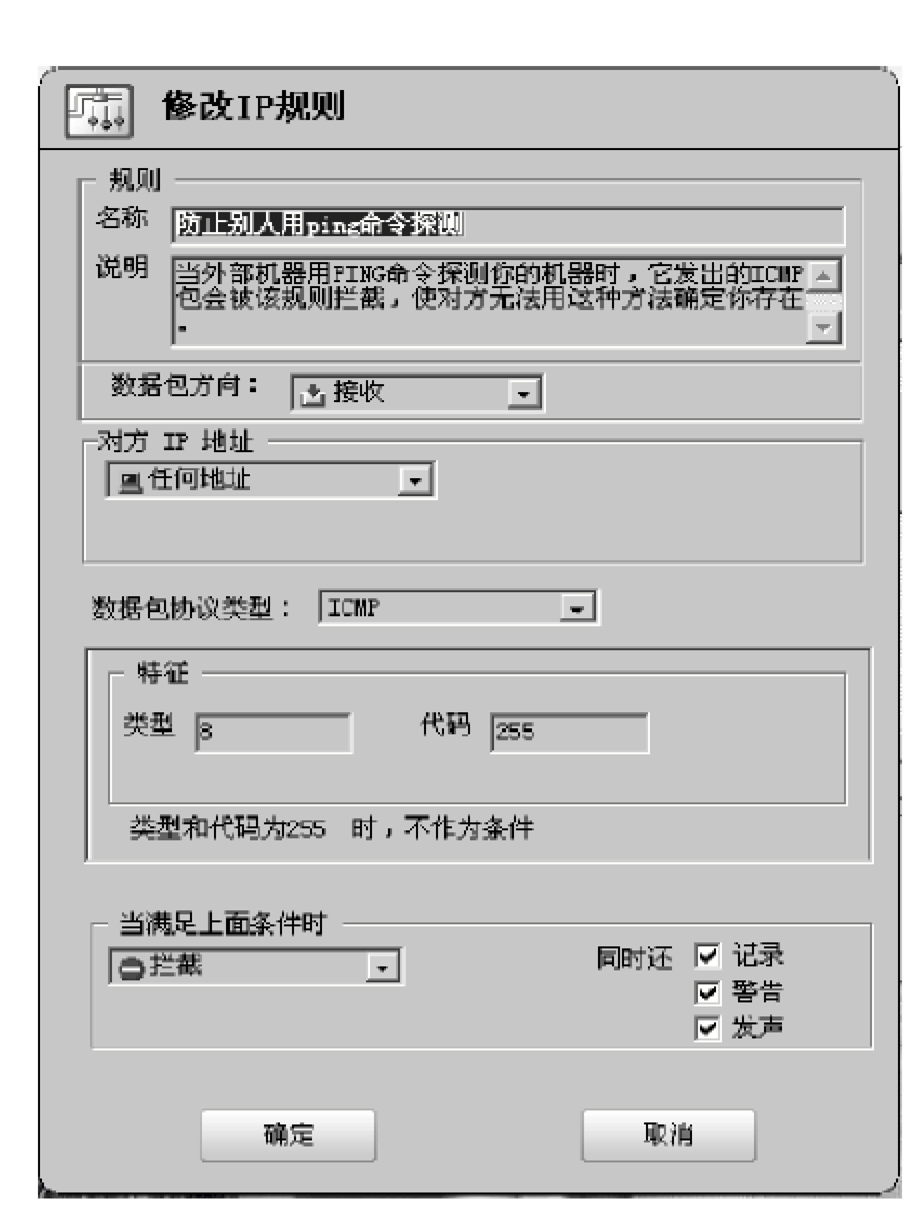


图 2.51　修改 IP 规则

（6）选择“应用程序规则”图标，选中窗口中某项应用程序打开设置对话框，对系统中应用程序访问网络权限进行设置，如图 2.52 和图 2.53 所示。



图 2.52　设置应用程序访问网络权限

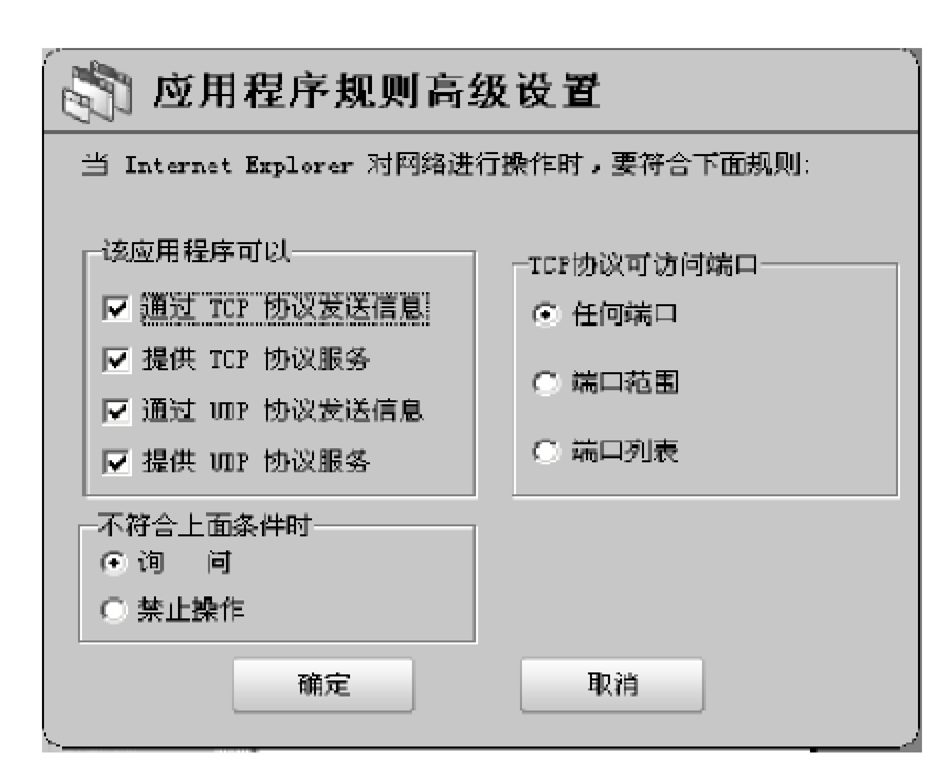


图 2.53　设置详细应用程序规则

（7）选择“系统设置”图标，打开配置窗口，在“基本设置”选项卡中，选中“开机后自动启动防火墙”复选框，如图 2.54 所示。

（8）打开“管理权限设置”选项卡，设置管理员密码，如图 2.55 和图 2.56 所示。



图 2.54　系统基本设置

图 2.55　设置管理权限

（9）打开“日志管理”选项卡，设置日志保存方式，如图 2.57 所示。

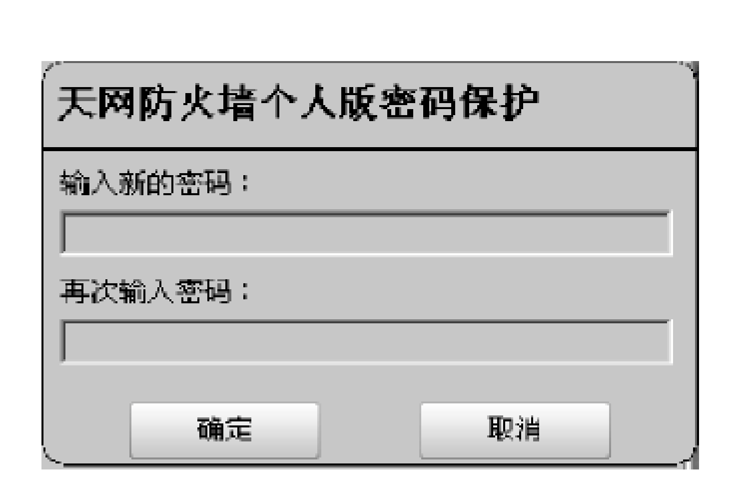


图 2.56　设置管理员密码



图 2.57　设置防火墙日志属性

（10）打开“入侵检测设置”选项卡，设置入侵检测功能，如图 2.58 所示。

（11）单击“应用程序网络使用情况”图标，查看系统相关网络应用程序使用网络端口的

情况，如图 2.59 所示。



图 2.58　设置入侵检测功能

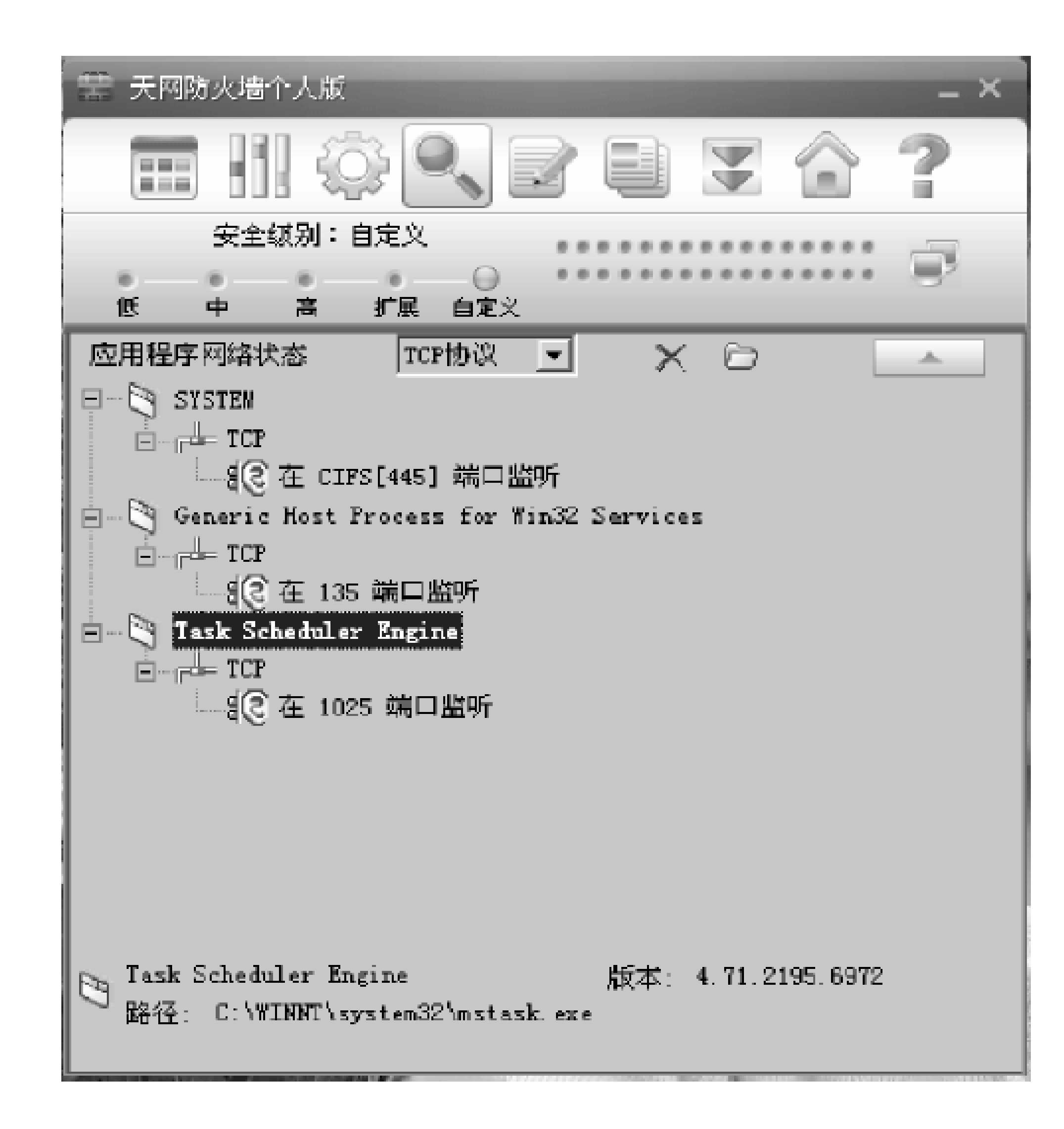


图 2.59　查看应用程序使用端口情况

（12）选择“日志”图标，查看详细防火墙日志记录，如图 2.60 所示。



图 2.60　查看防火墙日志

6. **实验报告与要求**

根据上面介绍的各项实验要求，详细观察记录防火墙配置前后的变化，两人一组考察防火墙设置对网络访问的影响，给出分析报告。

7. 实验分析与讨论

查阅资料，了解个人防火墙和企业级防火墙的区别。

8. 注意事项

（1）设置系统安全级别，如果选中“低”、“中”、“高”等级别，系统会自动完成对 IP 规则的设置，如果选中“自定义”，可以根据系统需要自行定义 IP 规则。

（2）进行安全设置时，大多数命令可以通过单击主界面上的图标实现，也可以通过右击桌面右下角的天网防火墙图标，选中相应菜单选项来打开设置功能。

第3章

计算机病毒防治

3.1 实验基础

3.1.1 计算机病毒概述

计算机病毒是一种人为制造的，侵入计算机系统、寄生于应用程序或系统可执行部分，并可以自我复制、传播，具有激活性、攻击性的程序代码。病毒是计算机技术发展的必然产物。病毒大多不以文件形式存在，寄生在合法程序上，可以是引导程序、可执行程序、Word文档等。

病毒的发展速度非常迅速。1980年IBM PC成为主流，其自身和DOS的弱点给病毒攻击造成可乘之机。1987年，实战病毒Brain出现。1988年底，首例在我国国家统计部门发现小球病毒感染。1992年，多态型病毒出现。1995年，出现能够变换自身代码的变形病毒。据统计，1989年1月计算机病毒种类不过100种，1990年1月已超过150种，1990年12月超过260种，目前计算机病毒总数超过6万，并以每天超过200个的速度诞生。

病毒有多种分类方法。按照传染目标可以分为引导型、文件型、混合型。按照破坏性可以分为良性病毒和恶性病毒。

病毒具有如下特征：刻意编写人为破坏、主动传染性、自我复制、扩散传播、隐藏性、可激活性、不可预见性。

计算机病毒可以通过不可移动的计算机硬件设备、移动存储设备、计算机网络、点对点通信系统和无线通信系统等多种途径进行传播。

计算机病毒程序是为了特殊目的而编制的，它通过修改其他程序而把自己复制进去，并且传染该程序。一般来说，计算机病毒程序包括三个功能模块：引导模块、传染模块和破坏模块。这些模块功能独立，同时又相互关联，构成病毒程序的整体。

引导模块的功能是借助宿主程序，将病毒程序从外存引进内存，以便使传染模块和破坏模块进入活动状态。另外，引导模块还可以将分别存放的病毒程序链接在一起，重新进行装配，形成新的病毒程序，破坏计算机系统。传染模块的功能是将病毒迅速传染，尽可能扩大染毒范围。病毒的传染模块由两部分组成：条件判断部分和程序主体部分，前者负责判断传染条件是否成立，后者负责将病毒程序与宿主程序链接，完成传染病毒的工作。病毒编制

者的意图，就是攻击破坏计算机系统，所以破坏模块是病毒程序的核心部分。破坏模块在进行各种攻击之前，首先判断破坏条件是否成立，只有条件全部满足时，破坏模块才开始其破坏活动。

现代计算机病毒具有以下流行特征：

(1) 攻击对象趋于混合型；

(2) 同时感染系统引导区和可执行文件；

(3) 采用反跟踪技术；

(4) 增强隐蔽性；

(5) 避开修改中断向量值，直接修改中断服务子程序；

(6) 请求在内存中的合法身份，通过正常的内存申请进行合法驻留；

(7) 维持宿主程序的外部特性，如控制文件显示属性或针对系统引导区的读操作提供正确内容给用户；

(8) 不使用明显的感染标志，使被感染文件的标志复杂化，难以识别；

(9) 病毒体繁衍不同变种。

目前杀毒软件中采用的技术主要有以下几种：

(1) 病毒扫描程序：在文件和引导记录中搜索病毒的程序。只能检测出它已经知道的病毒。操作简单，耗时，适用于简单病毒。

(2) 内存扫描程序：扫描内存以搜索内存驻留文件和引导记录中的病毒。发现后用一块未感染的软盘引导启动，病毒即被从内存清除。

(3) 完整性检查程序：计算机在未感染状态，取得每个可执行文件和引导记录的信息指纹，存放于硬盘的数据库中，用于验证原来记录的完整性。缺点是对已经被病毒感染的系统再使用这种方法，可能遭到蒙骗，不能对新文件进行有效的检查。

(4) 行为监视器：内存驻留程序，实时监测病毒和其他有恶意的损害活动并通知用户。可以防止新的、未知的病毒在计算机上传播。可能会影响一些活动与病毒相像的合法程序。不需要进行频繁的更新以保持有效。其缺点是无法监测出慢性病毒，因为这种病毒感染时不会主动调用系统服务。行为监视程序可以监测到的病毒种类有特定性。只有在病毒开始作用时，行为监视程序才能够监测病毒。

3.1.2 计算机病毒防治概述

防治计算机病毒应重在预防。一方面在思想上重视，管理上到位；另一方面依靠防杀计算机病毒软件。计算机病毒防治根本在于完善操作系统的安全机制。

单机用户进行病毒防范的简单有效的方法是选择一个功能完善的单机版计算机病毒软件，该软件应能满足：

- 拥有计算机病毒检测扫描器；
- 实时监控程序；
- 未知计算机病毒的检测；
- 压缩文件内部检测；
- 文件下载监视；

- 计算机病毒清除;
- 计算机病毒特征代码库升级;
- 重要数据备份;
- 定时扫描设定;
- 支持 FAT32 和 NTFS 等多种分区格式;
- 关机时检查软盘;
- 计算机病毒检测率较高。

个人用户还可以从以下方面进行病毒防护工作:

- 检查 BIOS 设置,将引导次序改为硬盘先启动;
- 安装较新的正式版本的防杀计算机病毒软件并经常升级;
- 经常更新计算机病毒特征代码库;
- 备份系统中重要的数据和文件;
- 在 Word 中,打开"提示保存 Normal 模板",将 Normal. dot 文件的属性改为只读;
- 对外来的光盘、软盘和下载的软件都应该先进行查杀病毒再使用;
- 启用防杀病毒软件的实时监控功能。

3.2 实验项目

3.2.1 宏病毒

1. 实验目的

理解宏病毒的概念、病毒机制、传播手段以及预防措施。

2. 实验原理

宏(Macro)是微软公司出品的 Office 软件包中所包含的一项特殊功能。微软公司设计此项功能的主要目的是给用户自动执行一些重复性的工作提供方便。它利用简单的语法,把常用的动作写成宏,用户工作时就可以直接利用事先编写好的宏自动运行,以完成某项特定的任务,而不必反复重复相同的工作。微软的 Word Visual Basic for Applications(VBA)是宏语言的标准。宏病毒正是利用 Word VBA 编写的一些宏,是一种寄存在文档或模板中的计算机病毒。一旦打开含有宏病毒的文档,其中的宏就会执行,宏病毒被激活,转移到计算机中并驻留在 Normal 模板上。以后所有自动保存的文档都会感染上这种宏病毒。

预防宏病毒有以下几种基本的方法。

(1) 防止执行自动宏:可以通过在 DOS 提示符下输入指令"WinWord. exe/m DisableAutoMacro"来防止打开 Word 文档时执行自动宏。另外,在打开或关闭文档时按下 Shift 键可以使文档不执行任何自动宏。

(2) 保护 Normal 模板:可以采取以下几种方法对 Normal 模板进行保护。提示保存 Normal 模板;设置 Normal 模板的只读属性;设置密码保护;设置安全级别;按照自己的习惯设置 Normal 模板并进行备份,当被病毒感染时,使用备份模板覆盖当前模板。

（3）使用 DisableAutoMacro 功能。

3. 实验环境

运行 Windows 操作系统的主机，安装 Windows Office 软件和 Windows Visual Studio 或者 Windows Visual Studio. Net 编程环境。

4. 实验内容

（1）手工创建一个 DOC 文档，在该文档的工程下增加一个宏病毒模块 VBS。

（2）观察执行下述动作后，哪些 Word 中已经存在 VBS：

① 新建一个文档，随机输入若干字符，然后关闭。

② 打开一个已经存在的文档，编辑若干字符，然后关闭。

③ 把上述两个文档复制到一个移动存储设备上，然后到另一台主机上去打开它们，然后关闭。

（3）按照宏病毒的预防方法配置主机，防范宏病毒攻击。

5. 实验步骤

（1）打开菜单项“工具”|“宏”|“录制新宏”，为文档添加新宏，如图 3.1 所示。

（2）打开菜单项“工具”|“宏”|“宏”，观察文档中包含的宏，如图 3.2 所示。





图 3.1　为文档添加新宏

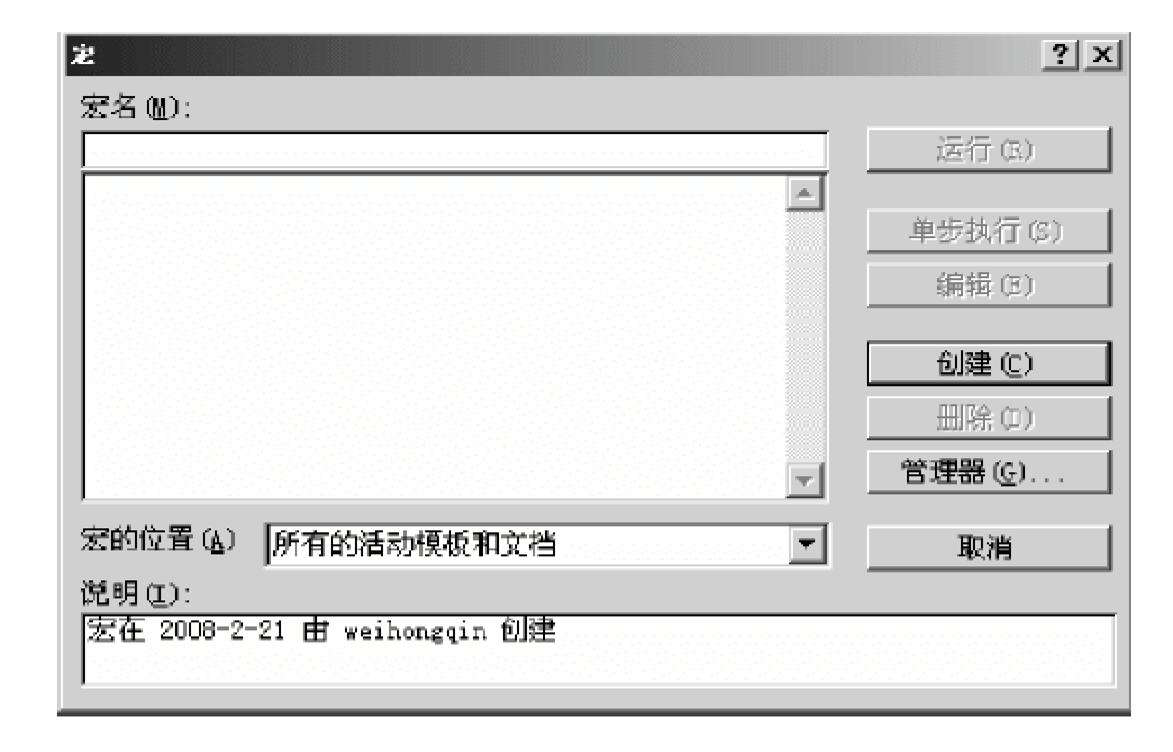


图 3.2　查看文档中包含的宏

（3）打开“工具”|“选项”|“安全性”，对它的属性进行安全设置，如图 3.3 和图 3.4 所示。

（4）在 Normal. dot 中增加 AutoExec 自动宏，使用 DisableAutoMacro 宏：

```
Sub AutoExec()
WordBasic.DisableAutoMacros True
End Sub
```

6. 实验报告与要求

根据上面介绍的各项实验要求，详细观察记录宏病毒执行感染前后的变化，给出分析报告。

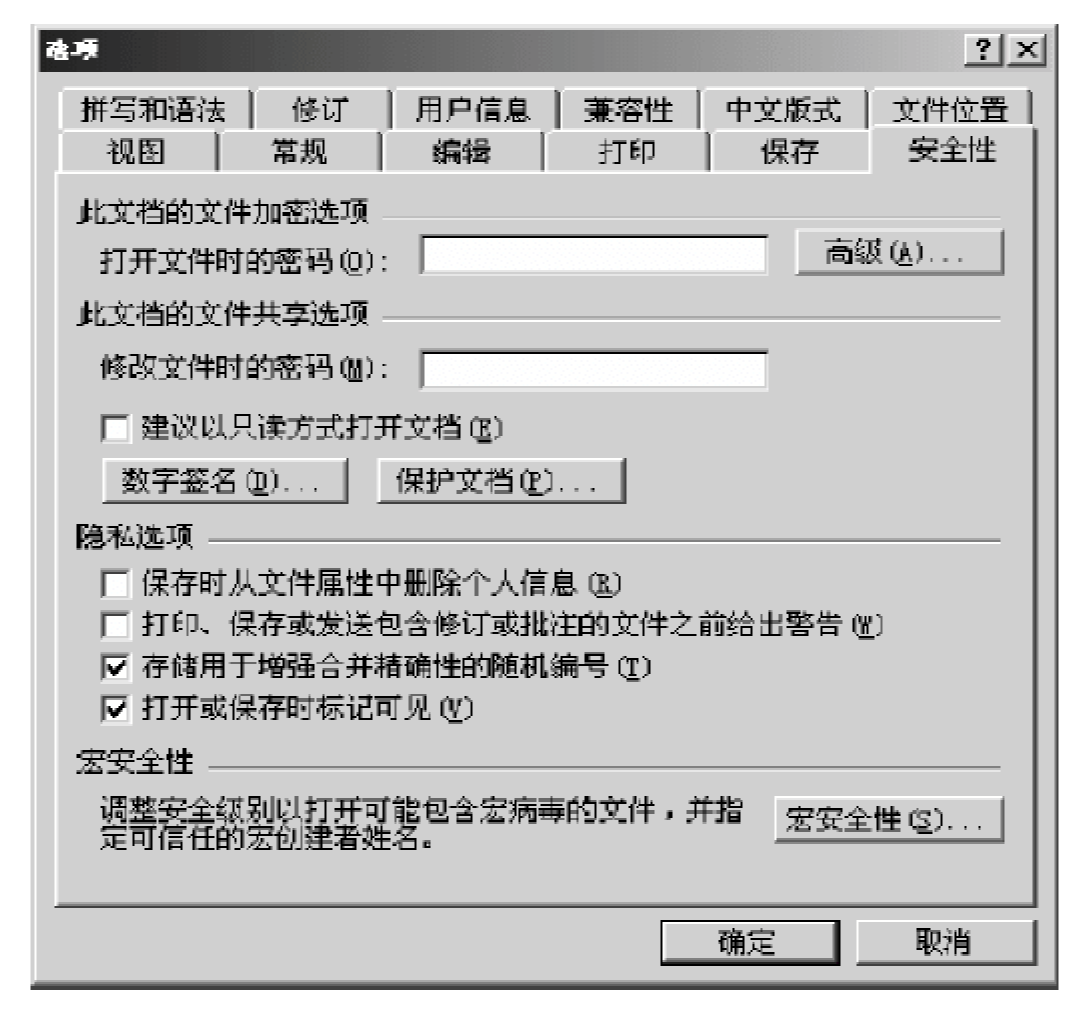


图 3.3　设置宏安全性

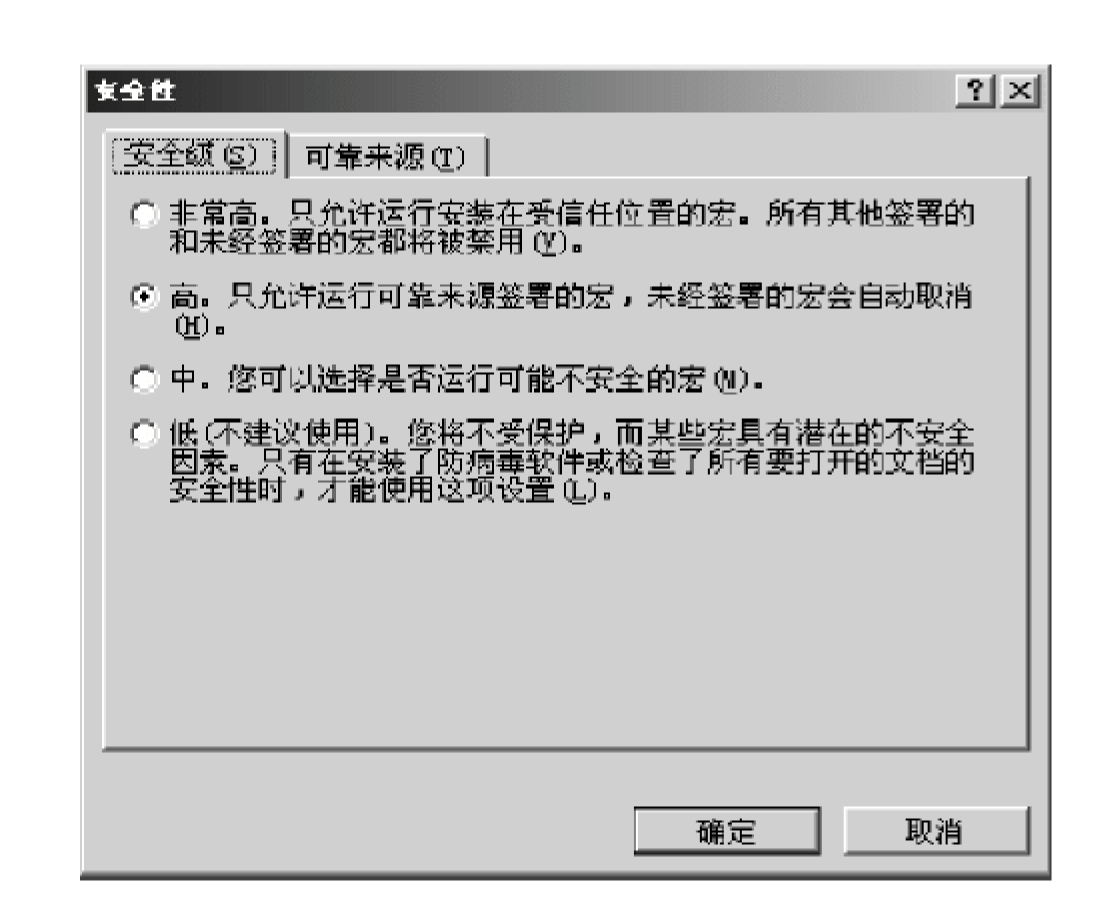


图 3.4　设置宏安全级别

7. 实验分析与讨论

脚本病毒的病毒原理、传播机制与宏病毒比较有何异同，如何进行防范。

8. 注意事项

禁止所有宏的执行可以从根本上防治宏病毒，但这是不现实的，因为用户有时需要使用自己编制的一些宏。禁止自动宏的执行，可以保证用户在安全启动 Word 文档后，进行必要的宏病毒检查，从而达到防治宏病毒的目的。

3.2.2　防病毒软件使用

1. 实验目的

了解防病毒软件基本工作原理，掌握防病毒软件配置和使用方法。

2. 实验原理

目前大多数防毒软件都提供了丰富的安全功能，不同的产品功能会有所不同。用户安装好防毒软件后，应了解其详细的使用方法，对其进行适当的设置，使之充分发挥作用，更好地满足个人的安全需求。

3. 实验环境

运行 Windows 操作系统的主机，安装 McAfee 的 VirusScan 反病毒软件。

4. 实验内容

（1）启用各监控模块；
（2）启用访问控制；
（3）更新病毒库并设置自动更新计划；
（4）对磁盘进行病毒扫描。

5. 实验步骤

（1）打开“VirusScan 控制台”对话框，对访问保护、缓冲区溢出保护、电子邮件扫描等功能进行启用，并打开各属性页进行设置，如图 3.5～图 3.10 所示。

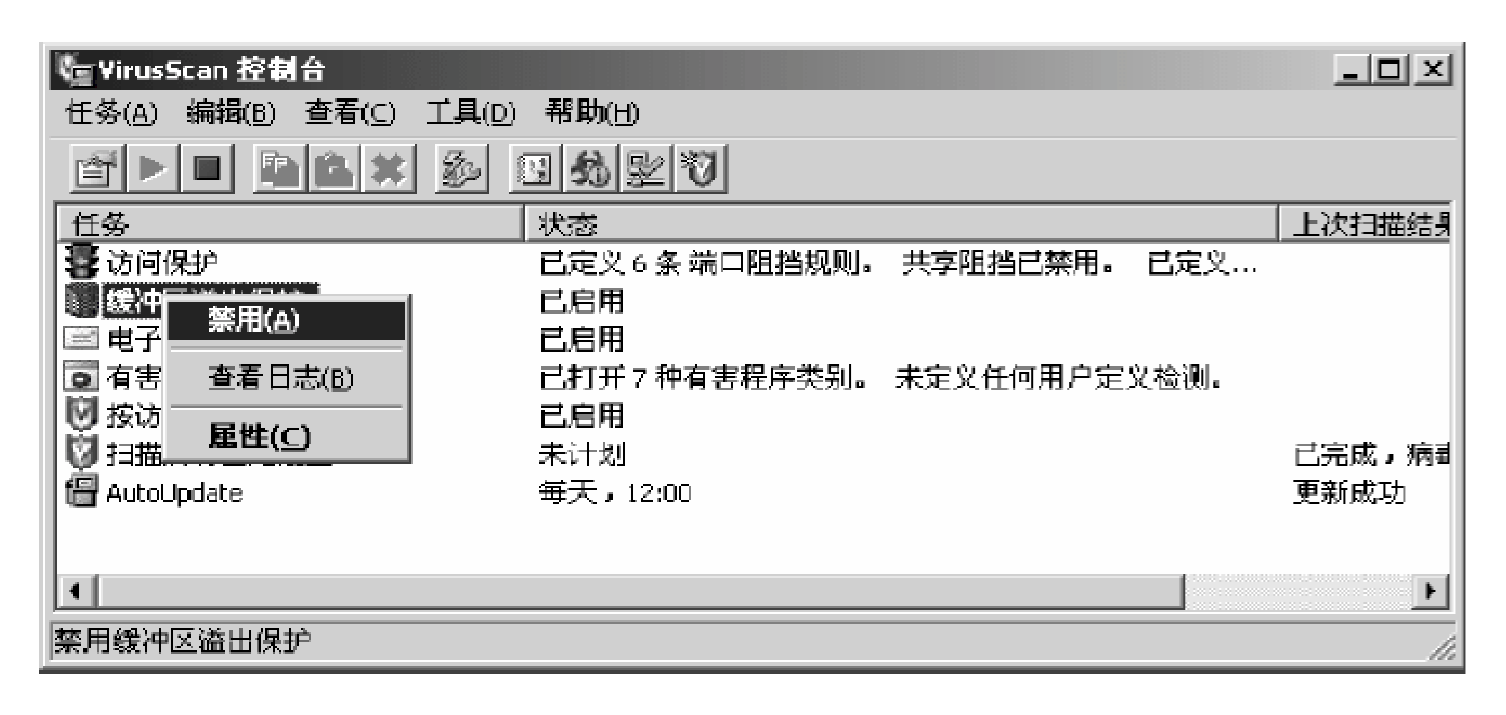


图 3.5 对防病毒软件各功能进行启用设置

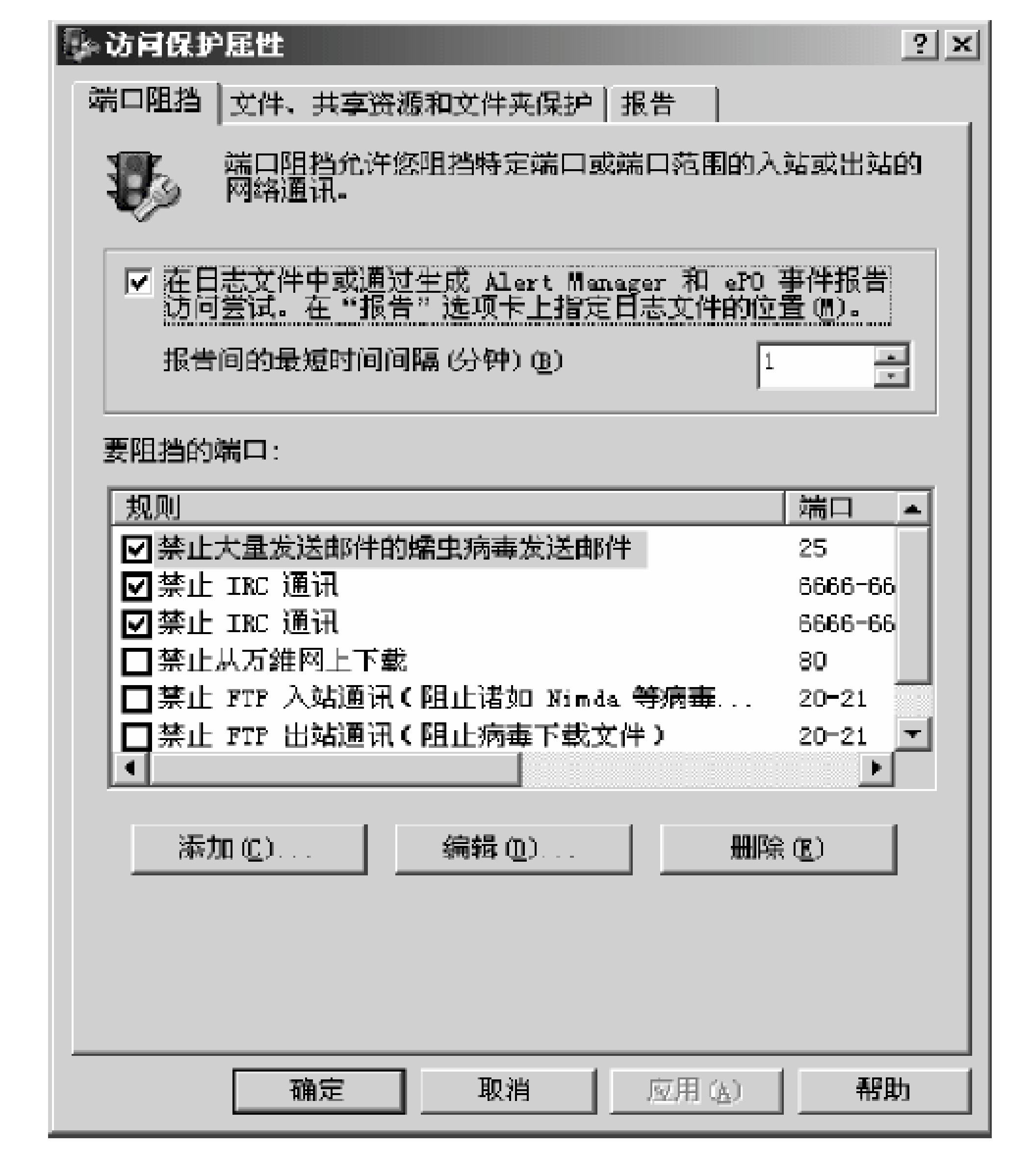


图 3.6 设置访问保护功能的端口阻挡属性

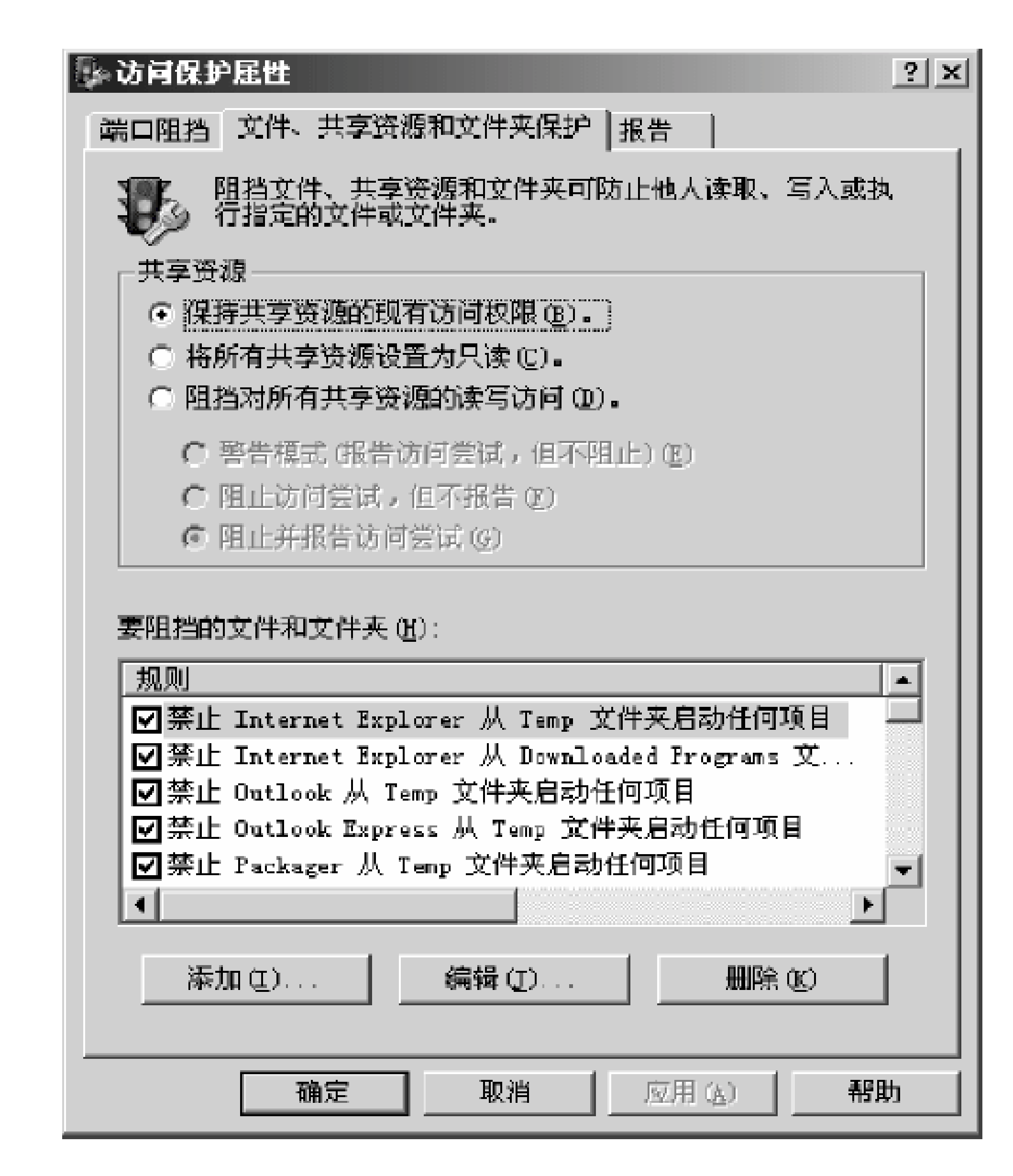


图 3.7 设置访问文件安全属性

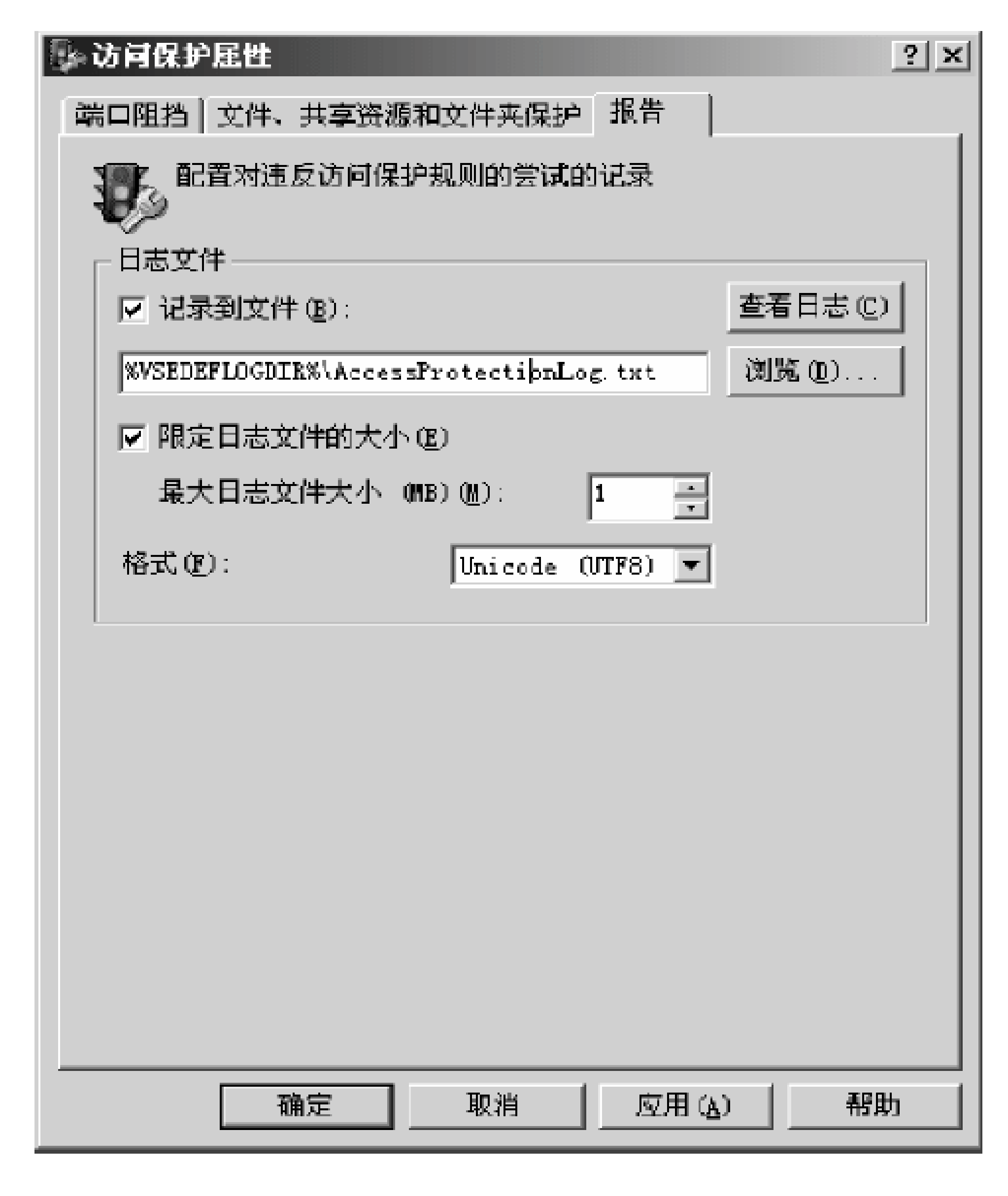


图 3.8 设置访问日志保护属性



图 3.9 设置缓冲区溢出保护属性

(2)"按访问扫描"是一种实时保护模块，用户应将其开启。可以在控制台窗口选中该模块右键选择"开启"选项，或者右击桌面右下角 VirusScan 图标，进行设置，如图 3.11 和图 3.12 所示。

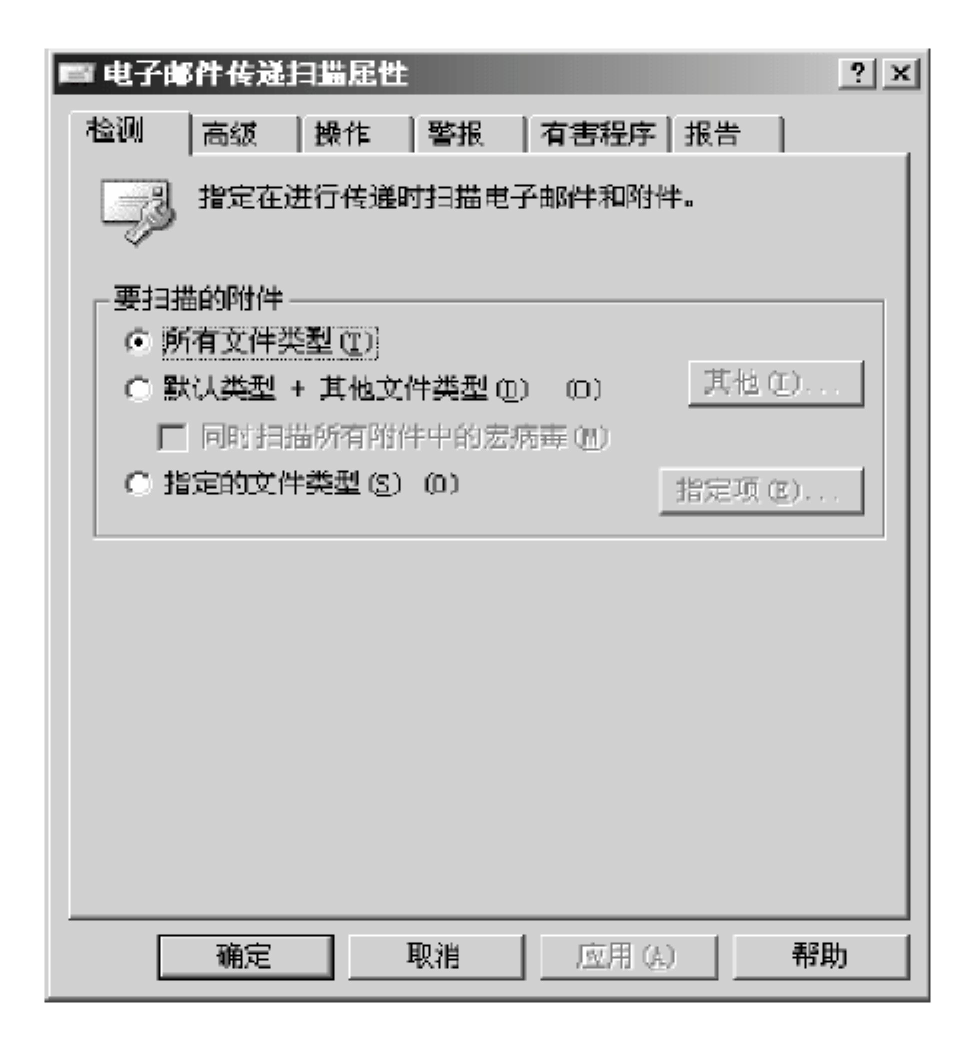


图 3.10 设置电子邮件扫描属性



图 3.11 设置按访问扫描属性

(3)打开 AutoUpdate 属性窗口，单击"立即更新"按钮，对杀毒软件和病毒库同时进行在线更新，单击"计划"按钮，可以制订更新计划，如图 3.13～图 3.15 所示。



图 3.12　设置按访问扫描计划



图 3.13　设置自动更新功能



图 3.14　设置自动更新计划

(4) 在控制窗口中打开，或右击桌面右下角 VirusScan 图标，选择“按需扫描…”选项，进行打开设置，如图 3.16 和图 3.17 所示。

6. 实验报告与要求

根据上面介绍的各项实验要求，使用杀毒软件对机器进行病毒查杀，详细观察记录执行结果，评价该杀毒软件的优缺点，提交分析报告。

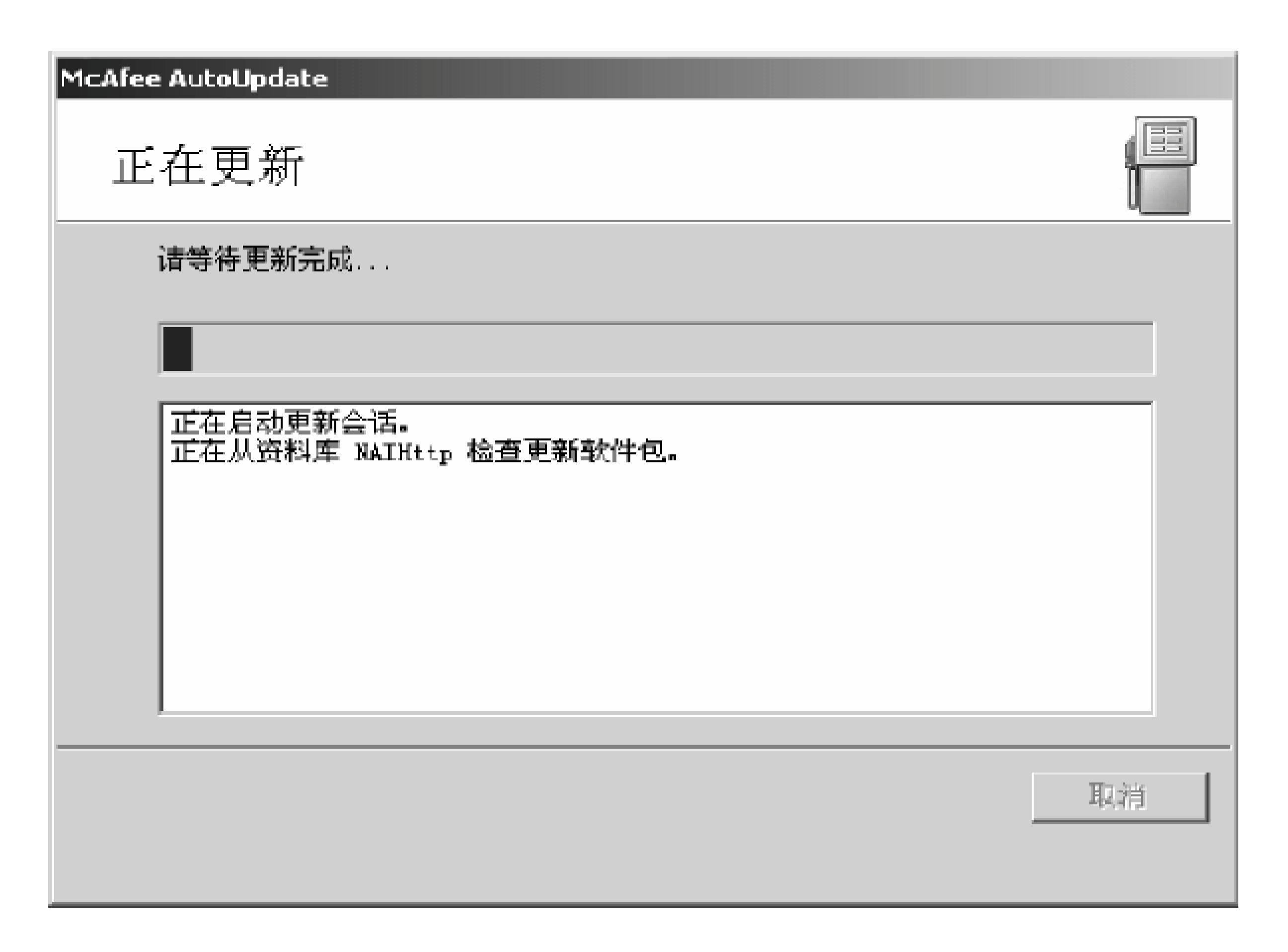


图 3.15 系统进行自动更新



图 3.16 启动按需扫描功能



图 3.17 对系统进行扫描

7. 实验分析与讨论

作为个人用户，除了使用防病毒软件，还应该采取哪些措施来防范病毒。市场上国内外商品化防毒软件很多，各种产品分别具有哪些特点，应该如何根据用户需要进行选择。

8. 注意事项

不同类型的防毒软件操作界面和使用方法都有不同，但核心功能是基本一致的。用户在使用不同的防毒软件时，可以首先从本实验提出的几个方面进行基本设置，同时考虑自己的需求对辅助功能模块进行选用。

第4章 应用系统安全

4.1 实验基础

4.1.1 鉴别与认证

鉴别与认证用于保证报文的完整性和不可否认性，分别可以通过报文鉴别和数字签名技术来实现。

报文鉴别通过鉴别函数实现。鉴别函数用于产生可以鉴别一个报文的值的鉴别符，有报文加密、报文鉴别码和散列函数三种形式。报文鉴别的基本工作原理为：假设通信双方A和B共享一个密钥K；当A要发送报文到B时，先利用密钥K计算MAC，然后将报文加上MAC发给B；B用相同的密钥对收到的报文执行相同的计算可以得到新的MAC，并与收到的MAC比较；如果B计算出的MAC与收到的MAC不同，则B知道攻击者已经更改了报文而未更改MAC(攻击者不知密钥)；如果B计算出的MAC与收到的MAC相同，则B可以确定报文来自A并且没有被更改。

数字签名可以同时鉴别报文内容和发送方、接收方身份。因此数字签名可以用来防止伪造、篡改信息或冒用别人名义发送信息，或发出(收到)信息后又加以否认等情况发生。为了达到这个目的，数字签名必须具有如下性质：

(1) 签名必须用可确定签名者的唯一信息，如签名者和签名时间可以证实；

(2) 签名之前必须能够鉴别报文的内容；

(3) 能被第三方验证以解决争端。

数字签名有多种分类方式：按照数字签名的实现可分为直接和需仲裁的数字签名；按照签名用户可分为单个用户签名和多个用户签名等。

(1) 直接数字签名：只涉及通信双方。发送方用自己的私钥加密整个报文，或加密报文的MAC值对报文签名；签名后，对整个报文和签名用接收方的公钥(非对称加密)或用双方共享的密钥(对称加密)再次进行加密，从而可以在提供签名的同时保证通信的机密性。直接数字签名存在的问题：有效性依赖于发送方私钥的安全性。发送方可能在发送消息后，声称其私钥被盗，进行发送行为的抵赖。

(2) 需仲裁的数字签名：可以解决直接数字签名存在的问题。A发给B的签名报文

(用 A 和 T 的会话密钥对签名加密)首先送到仲裁者 T 处,由 T 对报文及 A 的签名进行验证。然后 T 注明报文日期,加上一个报文已经过仲裁且属实的说明后发给 B。这样,A 就不能否认发送过该报文。关键是通信方必须充分信任仲裁。

需仲裁的数字签名既可以通过对称加密技术实现,也可以通过公开密钥技术实现。

对称密钥技术实现需仲裁的数字签名有两种方案。方案一:仲裁 T 能看到发送的报文。发送方 A 与仲裁 T 共享一个密钥 K_{AT},接收方 B 与 T 共享一个密钥 K_{BT}。方案二:仲裁 T 不能看到发送的报文。除了 K_{AT} 和 K_{BT},发送方 A 与接收方 B 还共享一个密钥 K_{AB}。

采用对称加密技术实现需仲裁的数字签名存在的问题为:仲裁可以和发送方联合否认一个签名的报文,或者和接收方联合起来伪造发送方的签名。非对称加密技术由于通信前各方没有共享任何信息,从而可以防止发生联合欺骗。

公开密钥技术实现需仲裁的数字签名的过程为:

(1) A 对报文 M 进行两次加密,先用私钥 K_{RA},再用 B 的公钥 K_{UB},得到一个有签名的机密报文;

(2) 再用 K_{RA} 加密 ID_A 和签名的报文,连同 ID_A 发给 T;

(3) T 能对外层加密进行解密,确信报文一定来自 A,但 T 不能解密内部经双重加密的报文;

(4) T 给加密报文加上时间戳,并用自己私钥加密,然后发送给 B;

(5) B 用 T 公钥解密,得到 ID_A、双重加密的报文和时间戳,再用 B 私钥和 A 公钥恢复报文 M。

为了满足特殊领域的应用需要,一些专用数字签名方案被提出,如带有时间戳的签名方案、盲签名方案、代理签名、团体签名、不可争辩签名方案、指定的确认者签名等。

凡是需要对用户的身份进行判断的情况都可以使用数字签名,如加密信件、商务信函、订货购买商品、远程金融交易、自动模式处理等。

4.1.2　公钥基础设施

公钥基础设施(Public Key Infrastructure,PKI)是利用公钥理论和技术建立的提供信息安全服务的基础设施。公钥体制是目前应用最广泛的一种加密体制,可以提供网络中信息安全的全面解决方案。采用公钥技术的关键是如何确认某个人真正的公钥。在 PKI 中,通过认证中心 CA 和“数字证书”来确认声称拥有公共密钥的人的真正身份。

数字证书是一个经证书认证中心 CA 数字签名的包含公开密钥拥有者信息以及公开密钥的文件。认证中心作为权威的、可信赖的、公正的第三方机构,专门负责为各种认证需求提供数字证书服务。认证中心颁发的数字证书均遵循 X.509 v3 标准,X.509 标准在编排公共密钥密码格式方面已被广泛接受。X.509 证书已被应用于许多网络安全协议,其中包括 IPSec、SSL、SET、S/MIME。

数字证书的格式在 ITU(国际电信联盟)制定的 X.509 v3 里定义,其中包括证书申请者的信息和发放证书 CA 的信息。

CA 的信息包含发行证书 CA 的签名和用来生成数字签名的签名算法,任何人收到证书后都能使用签名算法来验证证书是否是由 CA 的签名密钥签发的。任何想发放自己公钥

的用户，可以去认证中心申请自己的证书。CA 中心在认证该人的真实身份后，颁发包含用户公钥的数字证书。其他用户只要能验证证书是真实的，并且信任颁发证书的 CA，就可以确认用户的公钥。

PKI 是一种遵循标准的密钥管理平台，它能够为所有网络应用透明地提供采用加密和数字签名等密码服务所必需的密钥和证书管理。PKI 必须具有的基本成分包括：认证机关(CA)、证书库、密钥备份及恢复系统、证书作废处理系统、PKI 应用接口系统等。

目前世界上最权威的认证机构是美国的 VeriSign 公司。VeriSign 成立于 1995 年 4 月，是全球数字信任服务的主要提供商。它提供四种核心服务：网络服务、安全服务、支持服务以及电子交流服务，目的是创造一个诚信的环境，让企业和用户能够互相信任地进行商业往来和交流。世界 500 强企业全都在使用 VeriSign 的网络服务。国内的 CA 大致可以分为大行业或政府部门建立的 CA、地方政府授权建立的 CA 和商业性 CA 三类。目前国内的 CA 已经不是简单地提供证书，而是更多地开始为客户提供不同领域的解决方案，以及开发一些相关的安全系统。在技术上，也考虑采用了与国际标准相同的结构。此外，针对大家普遍关心的 CA 互通问题，也建立了一些有一定规模的 CA 联合体。

4.1.3 电子商务安全协议

常用的电子商务安全协议有电子邮件安全协议、电子商务交易安全协议(如 SSL 和 SET)等。

1. 电子邮件安全协议

在电子邮件安全中需要解决的问题有如下几方面。

(1) 发送者身份认证：如何证明电子邮件内容的发送者就是电子邮件中所声称的发送者；

(2) 不可否认：一旦发送了某封邮件，发送者就无法否认这封邮件是他发送的；

(3) 邮件的完整性：保证电子邮件的内容不被破坏和篡改；

(4) 邮件的保密性：防止电子邮件内容的泄漏。

通过采用安全电子邮件标准，配合传输层安全技术和邮件服务器的安全技术可以有效解决以上问题。目前有两套成型的端到端的安全电子邮件标准：PGP 和 S/MIME。

完善保密(Pretty Good Privacy，PGP)，最早版本于 1991 年发布，已在世界范围广泛使用，是目前最流行的电子邮件安全程序之一。PGP 可以在多种硬件平台上使用，它的使用相对比较容易。PGP 可为电子邮件提供多种安全功能，如保密性、信息来源证明、信息完整性、信息来源的无法否认性等。

PGP 中公钥本身的权威性可以由第三方，特别是收信人所熟悉或信任的第三方进行签名认证，没有统一的集中的机构进行公钥/私钥的签发。在 PGP 体系中，任意两方之间都是对等的，整个信任关系构成网状结构，即所谓的 Web of Trust，而且它工作时不需要有复杂的基础结构。比如 A 作为一个 PGP 用户，要对她知道是真实的钥匙给予证明。这些钥匙可以是她朋友的，同事的，或者她的亲戚的。在这些情况下，她可以起一个公证人的作用，在她知道是正确的证明上签上她的名字。PGP 证明上可以有多个机构证实它的有效性。这

里不存在某个每人都信任的证明机构，PGP用户依靠的是多个证明机构组成的巨大的机构网（信任网），每个机构都有一些人信任它。

S/MIME（Secure Multipurpose Internet Mail Extension）从PEM（Privacy Enhanced Mail）和MIME发展而来，同PGP一样，S/MIME也采用了单项散列算法和非对称的加密体系。S/MIME与PGP的主要不同体现在：

（1）认证机制依赖于层次结构的证书认证机构，即Tree of Trust；

（2）将信件内容签名加密后作为特殊的附件传送，证书格式采用X.509规范；

（3）侧重于作为商业和团体使用的工业标准，而PGP倾向于提供个人电子邮件的安全；

（4）支持的厂商相对较少。

2. SSL安全协议

安全套接层（Secure Socket Layer，SSL）协议是一个通过Socket层（传输层）对客户和服务器之间的事务进行安全处理的协议，适用于所有TCP/IP应用，由Netscape公司设计和开发。其目的在于提高应用层协议（如HTTP、Telnet和FTP等）的安全性。该协议已成为事实上的工业标准，网景、微软、IBM等公司已在使用该协议。

SSL协议的功能包括：

（1）数据加密；

（2）服务器验证；

（3）信息完整性；

（4）可选的客户TCP/IP连接验证。

在SSL协议中，双方开始通信之前，一方先提交给另一方自己的证书。得到公开密钥的一方先验证对方的身份，然后把自己的一些信息通过该密钥加密传送至另一方，通常这些信息是与会话密钥相关的，进而双方通过一定的算法生成会话密钥，握手阶段结束后便开始进行数据传输。

一个支持SSL的客户端软件通过下列步骤认证服务器的身份：

（1）从服务器传送的证书中获得相关信息；

（2）判别当天的时间是否在证书的合法期限内；

（3）签发证书的机关是否是客户端信任的；

（4）签发证书的公钥是否符合签发者的数字签名；

（5）证书中的服务器域名是否符合服务器真正的域名；

（6）服务器被验证成功，客户继续进行握手过程。

SSL协议中一般支付协议规定只需在会话的开始进行一次完整的握手过程，会话的其他连接可以使用第一次握手的加密算法和密钥等信息，以提高交易的速度。SSL用公开密钥加密，用来在客户与服务器之间交换一个进程密钥，这个密钥用来加密HTTP传输过程（包括请求和响应）。每次传输采用不同的密钥。

基于SSL的交易存在的问题有：

（1）SSL不能使客户确信SuperSoft接收信用卡支付是得到授权的。

（2）SSL除了传输过程外不能提供任何安全保证，黑客可能通过商家服务器窃取信用卡号。

（3）为了处理信用卡支付，几乎所有的商家都要求客户输入邮件地址。要求客户出示邮件地址是一种防止欺诈的措施，它必须与信用卡的帐单地址相符。但商店没有提供有关不得出卖该地址和不得在这次交易外使用该地址的承诺，因此顾客不能信任自己的隐私是否受到保护。

（4）SSL没有提供对浏览器用户的认证（可选）。

（5）通信过程没有数字签名，无法实现不可否认性。

3. SET协议

安全电子交易（Secure Electronic Transaction，SET）是一种基于消息流的应用层协议。用于保证在公共网络上进行银行卡支付交易的安全性，能够有效地防止电子商务中的各种诈骗。SET主要面向B2C模式，完全针对信用卡来制定，涵盖了信用卡在电子商务交易中的交易协定、信息保密、资料完整等各方面，并得到了大多数厂商的认可和支持。

SET核心技术包括公开密钥加密、数字签名、电子信封、电子安全证书等。SET交易分三个阶段进行：

（1）在购买请求阶段，用户与商家确定所用支付方式的细节；

（2）在支付的认定阶段，商家会与银行核实，随着交易的进展，他们将得到付款；

（3）在受款阶段，商家向银行出示所有交易的细节，然后银行以适当方式转移货款。

在SET协议中有持卡人、发卡机构、商家、银行、支付网关等角色。

（1）持卡人：通过计算机与商家交流，使用由发卡机构颁发的付款卡（如信用卡、借记卡）进行结算；

（2）发卡机构：通常为金融机构，为每一个建立了帐户的顾客颁发付款卡，发卡机构根据不同品牌卡的规定和政策，保证对每一笔认证交易的付款；

（3）商家：提供商品和服务，接受付款卡支付的商家必须和银行有关系；

（4）清算银行：在线交易的商家在银行开立帐号，并且处理支付卡的认证和支付；

（5）支付网关：可以由银行操作的、将Internet上的传输数据转换为金融机构内部数据的设备，也可以由指派的第三方处理商家支付信息和顾客的支付指令。

一个成功的SET交易的标准流程如下：

（1）客户在网上商店选中商品并决定使用电子钱包付款，商家服务器上的POS软件发报文给客户的浏览器要求电子钱包付款；

（2）电子钱包提示客户输入口令后与商家服务器交换握手信息，确认客户、商家均为合法，初始化支付请求和支付响应；

（3）客户的电子钱包形成一个包含购买订单、支付命令（内含加密了的客户信用卡号码）的报文发送给商家；

（4）商家POS软件生成授权请求报文（内含客户的支付命令），发给收单银行的支付网关；

（5）支付网关在确认客户信用卡没有超过透支额度的情况下，向商家发送一个授权响应报文；

（6）商家向客户的电子钱包发送一个购买响应报文，交易结束，客户等待商家送货上门。

SET 与 SSL 相比具有更强的功能，但提供这些功能的前提是：SET 要求在银行网络、商家服务器、顾客的 PC 上安装相应的软件，同时 SET 要求必须向各方发放证书。这些成为大面积推广 SET 的障碍，并且使得应用 SET 要比 SSL 昂贵得多。由于 SET 交易的低风险性以及各信用卡组织的支持，SET 将在基于 Internet 的支付交易中占据主导地位，但其普遍应用还需假以时日。

4.2　实验项目

4.2.1　OpenSSL 软件使用

1. 实验目的

掌握 OpenSSL 软件的下载、安装及部分功能的使用方法。更深一步理解加密技术和数字证书、CA、PKCS 标准、SSL 安全协议等概念，为以后可能在安全开发领域的发展奠定基础。

2. 实验原理

OpenSSL 软件是一个健全的、开放源代码的工具包，用于实现安全套接层协议（SSL v2/v3）和传输层安全协议（TLS v1）以及形成一个功效完整的通用加密库。该项目由全世界范围内志愿者组成的团体一起管理，他们使用 Internet 去交流、设计和开发这个 OpenSSL 工具和相关的文档。

OpenSSL 不但实现了 SSL 的一些接口，它所涵盖的内容从各种常用和标准的底层的对称、非对称加密算法到建立在其上的 PKI 的接口（包括 X.509 证书、PKI 标准、ASN.1 等）的实现一应俱全，并且还给出了一个有关 CA 的例子。OpenSSL 包由两部分组成：SSLeay 和 OpenSSL，前者是一套接口库，后者是建立在这个接口库之上的一个应用。用户可以通过使用 SSLeay 开发自己的应用，实现 SSL 的 128 位甚至更高位数的数据加密。随着时间的推移，OpenSSL 的功能越来越丰富。OpenSSL 可以被用作各种商业、非商业的用途，但是为了保护自由软件作者及其作品的权利，使用者在基于 SSLeay 和 OpenSSL 上作开发时，需要遵守一些相关协定。

3. 实验环境

一台安装 Windows 2000/XP 操作系统的计算机。

4. 实验内容

（1）了解并下载安装 OpenSSL 软件；
（2）利用 enc 命令进行对称加密/解密；
（3）利用 gendsa 和 genrsa 来产生不对称密钥对；

（4）利用 rsautl 来进行数据加密/解密、签名和身份验证；

（5）利用 OpenSSL 生成证书；

（6）证书内容查看和使用。

5. 实验步骤

1）OpenSSL 软件了解及下载安装

（1）阅读相关帮助文档，初步了解 OpenSSL 软件。

（2）从 www.openssl.org 网站下载相应平台下的 OpenSSL 压缩软件包，解压缩到某个目录下（如 d:\openssl），如图 4.1 所示。

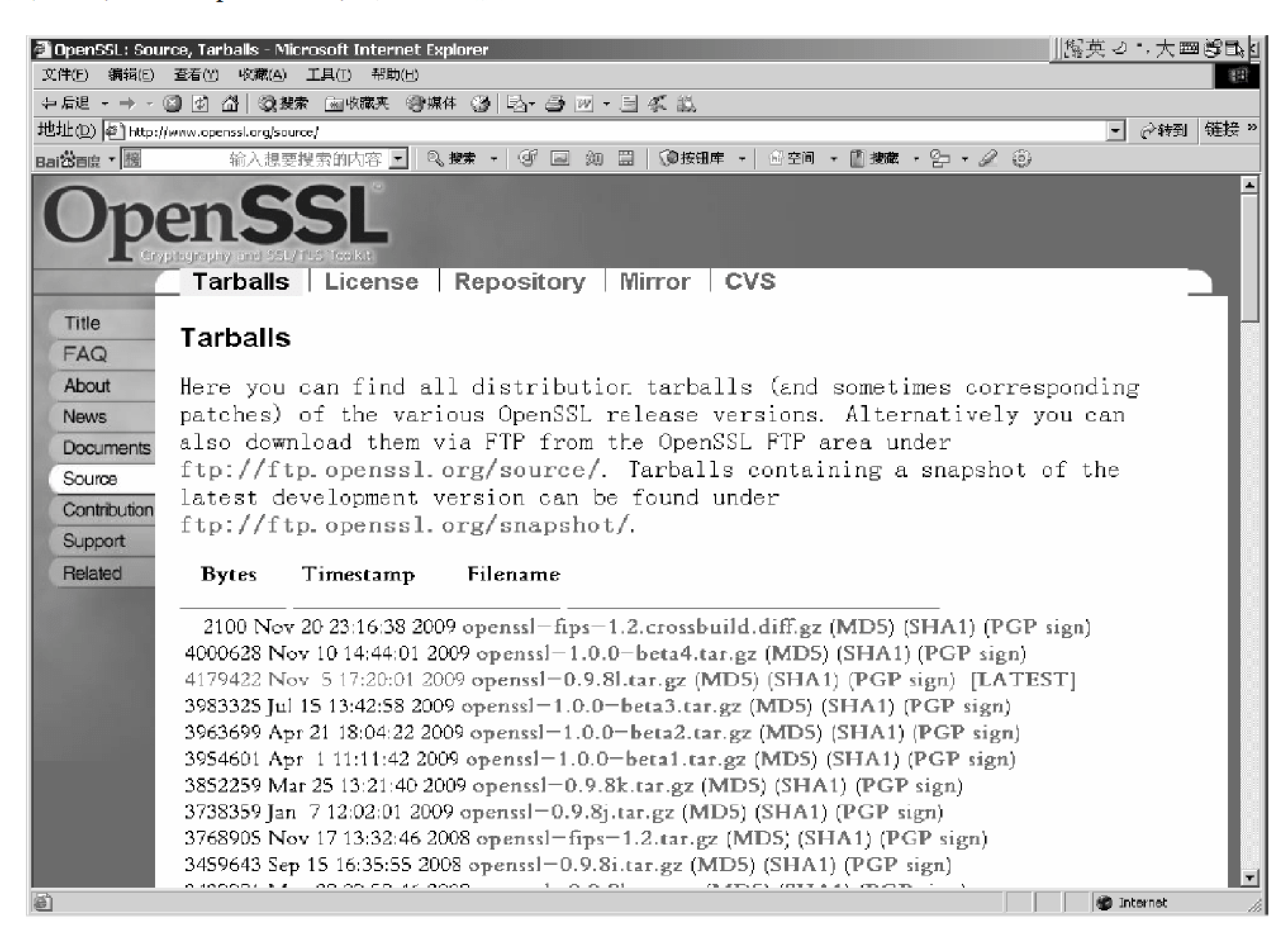


图 4.1　OpenSSL 软件包下载网站

（3）安装 Perl 编译环境（初始化的时候，需要用到 Perl 解释器）ActivePerl-5.6.1.629-MSWin32-x86-multi-thread.msi（安装时，选择“配置环境变量”），如图 4.2 和图 4.3 所示。

（4）安装 C 编译器 Visual C++软件。安装时选择“自动配置环境变量”，如果没有配置变量，在安装后可在 C:\Program Files\Microsoft Visual Studio\VC98\bin 目录（默认安装时）下执行 vcvars32.bat 以配置环境变量，OpenSSL 编译时需要用到 VC 自带的命令。

（5）运行 DOS 控制台程序，执行配置文件 Configure，如图 4.4 所示，进行环境变量设置，执行步骤为：

```
d:\openssl>perl Configure VC-WIN32
d:\openssl>ms\do_ms
```



图 4.2　安装 Perl 编译环境

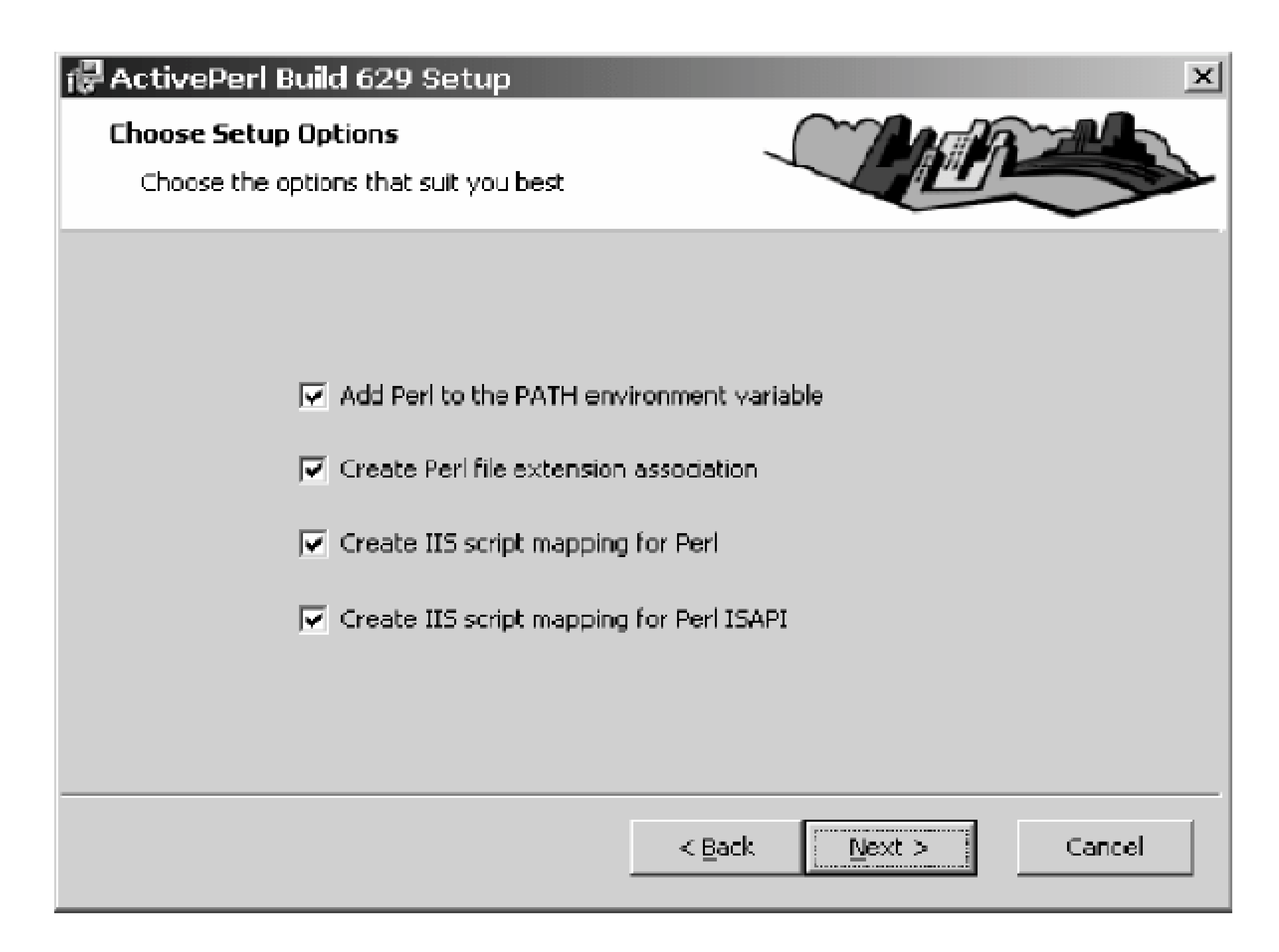


图 4.3　配置 Perl 环境变量

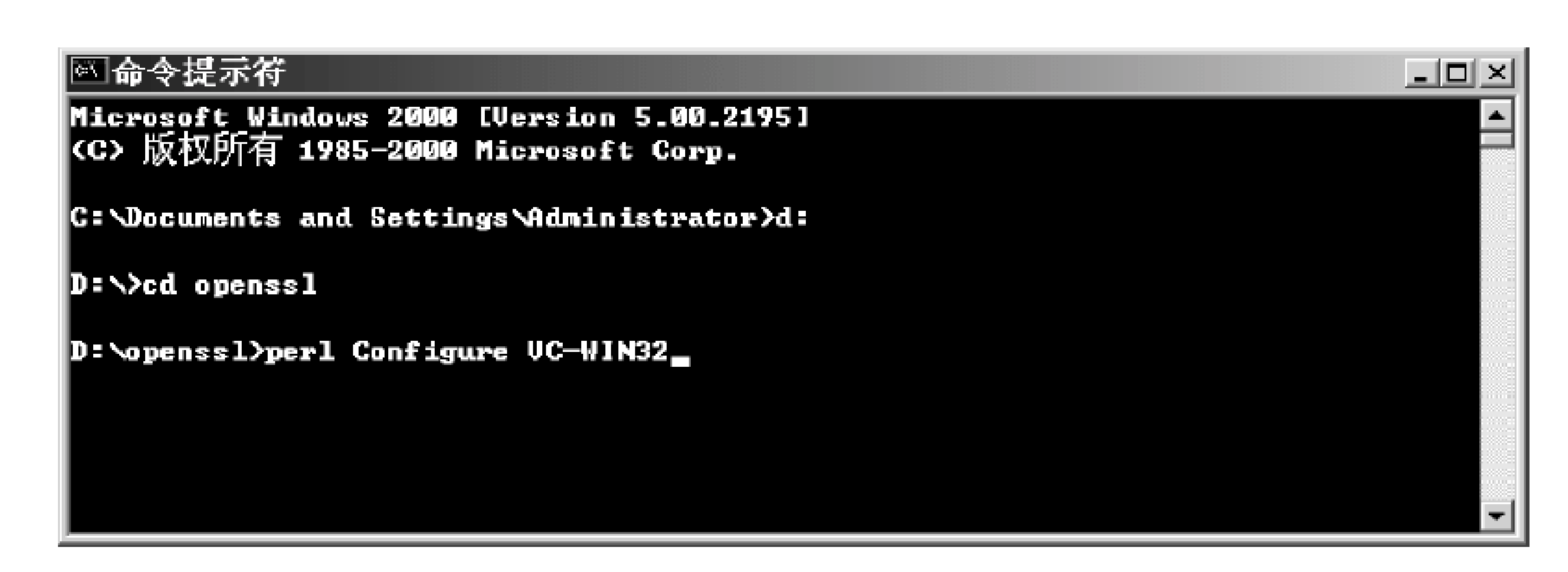


图 4.4　安装初始化配置

（6）编译 OpenSSL 软件，执行命令 d:\openssl>nmake -f ms\ntdll.mak，成功后将会在 d:\openssl 下生成 out32dll 目录，目录中存有 OpenSSL 相关的 DLL 文件和 EXE 文件。

（7）测试 OpenSSL 软件，测试步骤为：

```
d:\openssl>cd out32dll
d:\openssl\out32dll>..\ms\test
```

如果以上各步骤都没有出错信息，则表明 OpenSSL 软件已成功安装。

2）利用 enc 命令进行对称加密/解密

（1）把某文件转换成 Base64 编码方式：

① 用记事本在 openssl 目录下生成一个文件 file. bin；

② 运行命令 openssl enc -base64 -in file. bin -out file. b64；

③ 查看 file. b64 文件。

（2）把某 Base64 编码文件转换成源文件：

① 删除 openssl 目录下的 file. bin 文件；

② 运行命令 openssl enc -base64 -d -in file. b64 -out file. bin；

③ 查看 openssl 目录下的 file. bin 文件。

3）把某文件用 DES-CBC 方式加密和解密

操作方法同 enc 方式，命令分别为：

```
openssl enc －des3 －in file.txt －out file.des3
openssl enc －des3 －d －in file.des3 －out file.txt
```

4）利用 gendsa 和 genrsa 来产生不对称密钥对

（1）产生一个 1024 位长的 DSA 私钥，命令为：

```
openssl dsaparam －rand －genkey －out mydsa.key 1024 (dsaparam 命令产生 DSA 参数)
openssl gendsa －des3 －out mydsaCA.key mydsa.key (gendsa 命令产生 DSA 的不对称密钥)
```

（2）产生一个 1024 位长的 RSA 私钥，命令为：

```
openssl genrsa －des3 －out myrsaCA.key 1024
```

5）利用 rsautl 来进行数据加密/解密、签名和身份验证

（1）用公钥对文件加密：openssl rsautl -encrypt -in aa. txt -inkey myrsaCA. key -out aaenc. txt

（2）用私钥对文件解密：openssl rsautl -decrypt -in aaenc. txt -inkey myrsaCA. key -out aanew. txt

（3）用私钥对文件签名：openssl rsautl -sign -in aa. txt -inkey myrsaCA. key -out sig

（4）用公钥对签过名的数据进行验证，得到原来的数据：openssl rsautl -verify -in sig -inkey myrsaCA. key -out aa_priv. txt

6）利用 OpenSSL 生成证书

（1）在 openssl 目录下创建一个子目录，如 mytest，在此目录下编辑一个配置文件 openssl. cnf，内容如下：

```
[ req ]
default_bits = 1024
default_keyfile = ca.key
```

```
distinguished_name = req_distinguished_name
x509_extensions = v3_ca
string_mask = nombstr
req_extensions = v3_req

[req_distinguished_name ]
countryName = Country Name (2 letter code)
countryName_default = CN
countryName_min = 2
countryName_max = 2
stateOrProvinceName = State or Province Name (full name)
stateOrProvinceName_default = Shanghai
localityName = Locality Name (e.g., city)
localityName_default = Shanghai changning
0.organizationName = Organization Name (e.g., company)
0.organizationName_default = My Directory DHU
organizationalUnitName = Organizational Unit Name (e.g., section)
organizationalUnitName_default = Certification Services Division
commonName = Common Name (e.g., DHU Root CA)
commonName_max = 64
emailAddress = Email Address
emailAddress_max = 40

[v3_ca]
basicConstraints = critical,CA:true
subjectKeyIdentifier = hash

[v3_req]
nsCertType = objsign,email,server

[ ca ]
default_ca = default_CA

[default_CA ]

dir             = .                 # Where everything is kept
certs           = $dir              # Where the issued certs are kept
crl_dir         = $dir              # Where the issued crl are kept
database        = $dir/index.txt    # database index file.
unique_subject  = no                # Set to 'no' to allow creation of
                                    # several ctificates with same subject.
new_certs_dir   = $dir              # default place for new certs.

certificate     = $dir/cacert.crt   # The CA certificate
serial          = $dir/serial       # The current serial number
private_key     = $dir/ca.key       # The private key

#crlnumber      = $dir/crlnumber    # the current crl number
                                    # must be commented out to leave a V1 CRL
#crl            = $dir/crl.pem      # The current CRL
#RANDFILE       = $dir.rand         # private random number file
```

```
default_days = 365
default_crl_days = 30
default_md = md5
preserve = yes
x509_extensions = user_cert
policy = policy_anything

[policy_anything ]
commonName = supplied
emailAddress = supplied

[user_cert ]
#SXNetID = 3:yeak
subjectAltName = email:copy
basicConstraints = critical,CA:false
authorityKeyIdentifier = keyid:always
extendedKeyUsage = clientAuth,emailProtection
```

(2) 从 openssl\out32dll\demoCA 目录下复制以下几个文件到当前目录：

```
index.txt
serial
cacert.srl
```

(3) 为 CA 创建一个 RSA 私钥：

```
set path=d:\openssl\out32dll;%path%;
```

设置 OpenSSL 命令所在的默认路径，也可直接在系统环境变量中进行添加修改

```
openssl genrsa -des3 -out ca.key 1024
```

(4) 根据提示输入保护密码，将在当前目录下生成 ca.key 私钥文件。

(5) 利用 CA 的 RSA 私钥创建一个自签名的 CA 根证书：

```
openssl req -new -x509 -days 3650 -key ca.key -out cacert.crt -config openssl.cnf
```

(6) 输入命令后，提示输入国家代号、省份名称、城市名称、公司名称等，生成的根证书的名字为 cacert.crt。

(7) 为客户颁发证书：

```
openssl genrsa -des3 -out user.key 1024
openssl req -new -key user.key -out user.csr -config openssl.cnf
openssl x509 -req -in user.csr -out user.crt -CA cacert.crt -CAkey ca.key -days 600
```

(8) 根据提示输入一些个人信息，生成客户证书 user.crt。

(9) 可进一步将客户证书 user.crt 转换为个人私钥证书：

```
openssl pkcs12 -export -clcerts -in user.crt -inkey user.key -out user.p12
```

(10) 使用 CA 命令来模拟 CA 中心，进行证书签发：

```
openssl ca -config openssl.cnf -in user.csr -out newuser.crt
```

7）证书内容查看和使用

（1）显示 user.crt 中的内容：

```
openssl x509 -in user.crt -noout -text
```

（2）复制出 user.crt 中的公钥，放在文件 userpub.key 中：

```
openssl x509 -in user.crt -pubkey -noout>userpub.key
```

（3）对签名的证书 user.crt 进行详细分析：

```
openssl asn1parse -in user.crt
```

（4）将根证书和客户证书分别导入 IE 和 Outlook 中进行安全电子邮件的发送。

6. 实验报告与要求

根据上面介绍的各项实验要求，了解并使用 OpenSSL 软件的各项功能，并模拟一个根 CA 为指导教师颁发一张客户证书，用该公钥给教师发送一封加密邮件，将根证书和客户证书（带私钥）文件作为邮件附件一起发出。

7. 实验分析与讨论

OpenSSL 软件提供了从底层各种加密算法到应用层 CA 的实现方法，用户可以结合自己所掌握的密码学知识对 OpenSSL 中本实验未涉及的功能进行尝试，并考虑如何利用 OpenSSL 提供的功能实现其他高层的应用开发。

8. 注意事项

（1）安装 OpenSSL 软件包时，如果实验计算机上已安装 VC6.0，但没有配置变量，可以运行 vcvars32.bat 然后重启或者手工添加相关的环境变量，添加方法为进入“控制面板”|“系统”|“高级”|“环境变量”，在系统变量中加入下列内容：

① Path 变量：“c:\Program Files\Microsoft Visual Studio\Common\MSDev98\Bin;c:\Program Files\Microsoft Visual Studio\Common\Tools;c:\Program Files\Microsoft Visual Studio\VC98\bin”。

② MSDevDir 变量：“c:\Program Files\Microsoft Visual Studio\Common\MSDev98”。

③ Include 变量：“c:\Program Files\Microsoft Visual Studio\VC98\atl\include;c:\Program Files\Microsoft Visual Studio\VC98\mfc\include;c:\Program Files\Microsoft Visual Studio\VC98\include”。

④ Lib 变量：“c:\Program Files\Microsoft Visual Studio\VC98\mfc\lib;c:\Program Files\Microsoft Visual Studio\VC98\lib”。

需要注意的是，以上内容对于已有变量为添加进去，不是替换，原有信息部分仍然保留；对于未有变量，需要新建。

（2）enc 命令的详细参数说明见相关帮助文档，或在命令行输入“openssl enc -help”了解各参数含义和取值方法，其他命令同。

（3）建议用户将练习相关的文件放入一新建的文件夹中，如 mytest，要在其他目录中

使用 out32dll 中的命令，需要把 d:\openssl\out32dll 路径加入 Path 环境变量中。

（4）利用 rsautl 来进行数据加密/解密时，只能对少量数据（一般少于 150 字节）进行。

（5）在 Windows 2000 Server 下，不需要重新安装 OpenSSL 软件，只需要从教师机上下载 OpenSSL 的执行版，解压缩到 D 盘根目录下，将文件夹名改成 openssl。另外，使用软件前需要安装 Perl 编译环境 ActivePerl-5.6.1.629 -MSWin32 -x86 -multi -thread.msi。

（6）在 IE 和 Outlook 中使用 OpenSSL 所产生的证书时，方法参照实验“数字证书的申请与使用”。

4.2.2 SSL 安全协议

1. 实验目的

通过实验掌握利用 Windows 2000 的证书服务在网络中实现 SSL 安全连接，用 HTTPS 协议代替 HTTP 协议，实现安全的 Web 传输。

2. 实验原理

目前 Web 浏览器普遍将 SSL 与 HTTP 协议相结合来保证两个应用间通信的保密性和可靠性，以解决 Web 上信息传输的安全问题。SSL 位于七层网络模型的会话层，与应用层协议独立无关，因此，高层的应用层协议能透明地建立于 SSL 协议之上，SSL 协议在应用层协议通信之前就已经完成加密算法、通信密钥的协商以及服务器认证工作。基于 SSL 的通信中，服务器端的认证是必需的，客户端的认证是可选的，也可以通过对网站安全属性进行设置强制要求客户端认证，实现通信双方的身份认证。

3. 实验环境

服务器端是运行 Windows 2000 Server 操作系统的计算机，客户端是运行 Windows 2000 Professional 操作系统的计算机，服务器端已安装 IIS 服务组件。

4. 实验内容

（1）在 Windows 2000 Server 上安装证书服务；

（2）Web 网站申请证书；

（3）CA 机构颁发证书；

（4）Web 网站下载、安装 CA 颁发的证书。

5. 实验步骤

1）在 Windows 2000 Server 上安装证书服务

（1）选择“开始”|“设置”|“控制面板”，打开控制面板窗口，选择“添加”|“删除程序”窗口中的“添加”|“删除 Windows 组件”图标，在“Windows 组件向导”对话框中选择“证书服务”，如图 4.5 所示。

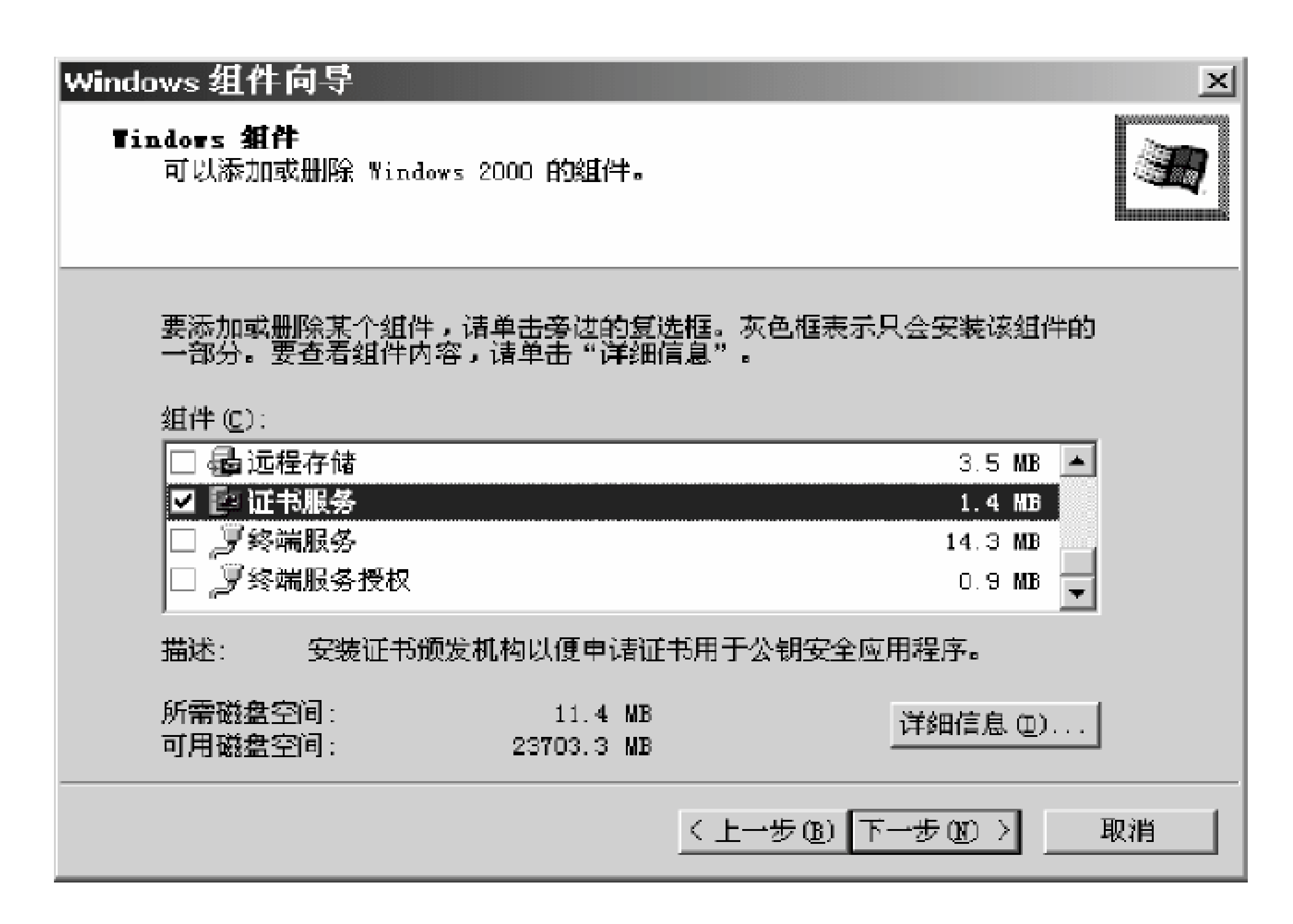


图 4.5 安装证书服务

(2) 在出现的提示框中单击"是"按钮，如图 4.6 所示。

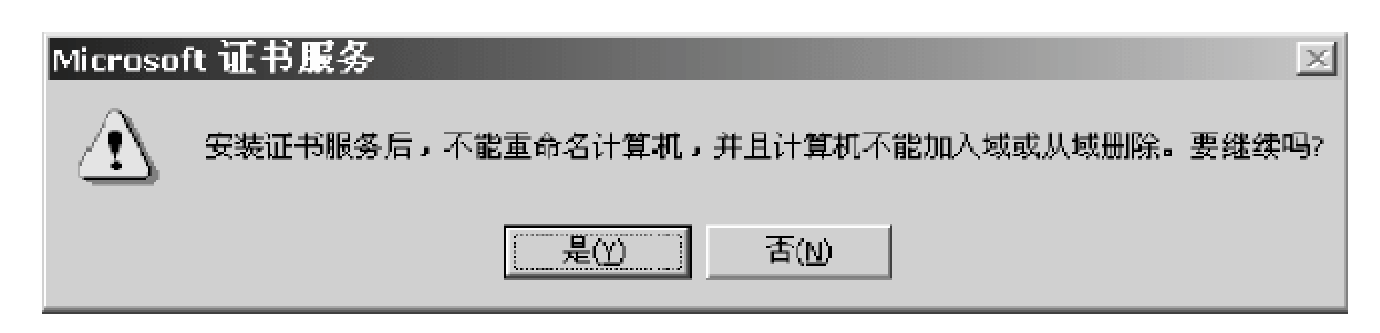


图 4.6 确认安装证书服务

(3) 选择"独立根 CA"单选按钮，如图 4.7 所示。

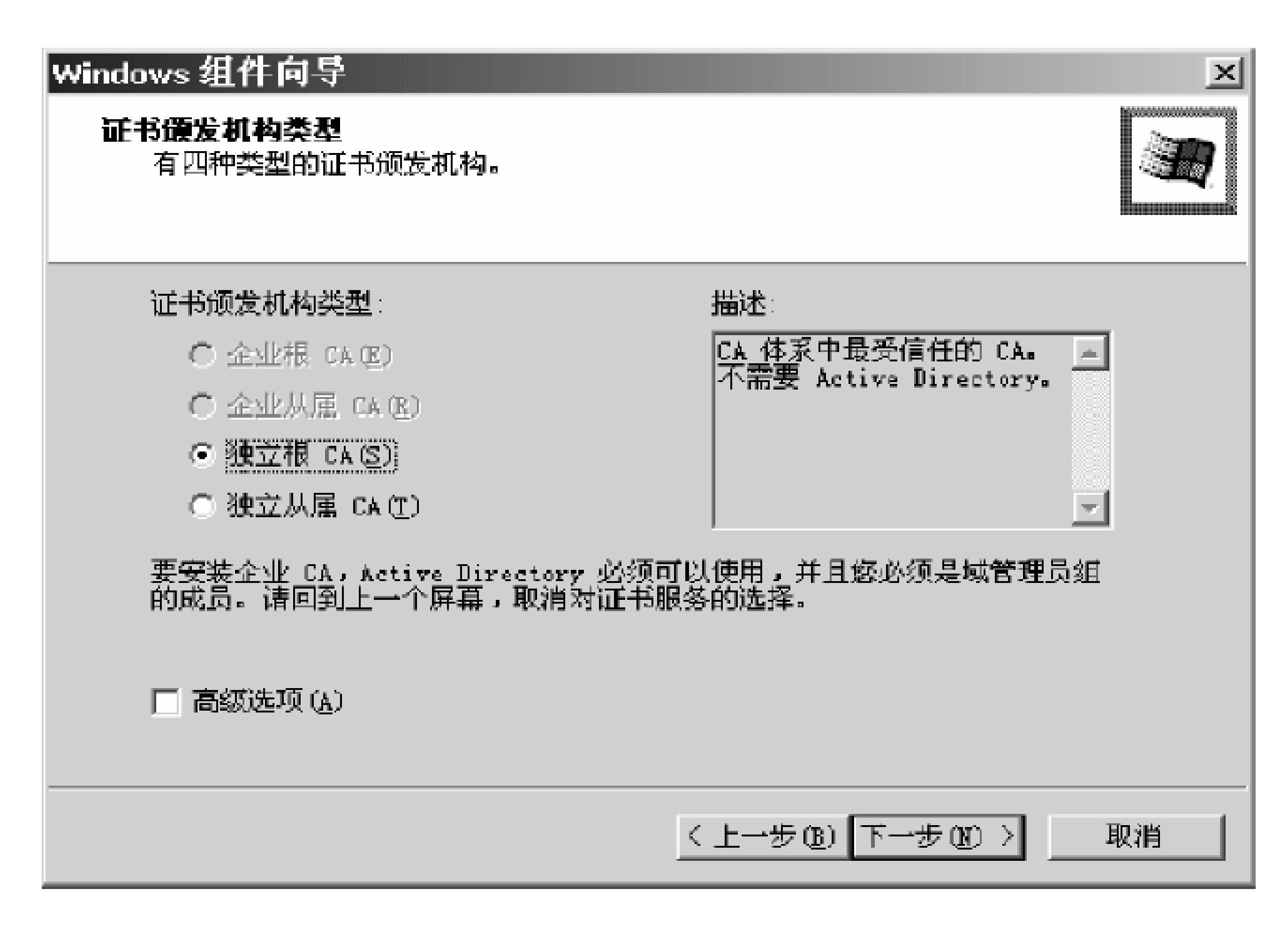


图 4.7 选择证书颁发机构类型

(4) 输入 CA 注册信息，如图 4.8 所示。

(5) 确定 CA 证书数据库、数据库日志及共享文件夹的存放位置，如图 4.9 所示。



图 4.8 输入注册信息



图 4.9 设置相关文件存放位置

(6) 在 CA 安装过程中，需要停止 IIS 服务，如图 4.10 和图 4.11 所示，安装成功后，IIS 服务和证书服务会自动启动。



图 4.10 停止 IIS 服务

2) Web 网站服务器证书申请

(1) 选择“开始”|“程序”|“管理工具”|“Internet 服务管理器”命令，在打开的窗口中选中默认 Web 站点，右击鼠标，在弹出的快捷菜单中选择“属性”命令，如图 4.12 所示。

(2) 在站点属性对话框中，选择“目录安全性”选项卡，单击“服务器证书”按钮，如图 4.13 所示。启动 Web 服务器证书向导，如图 4.14 所示。

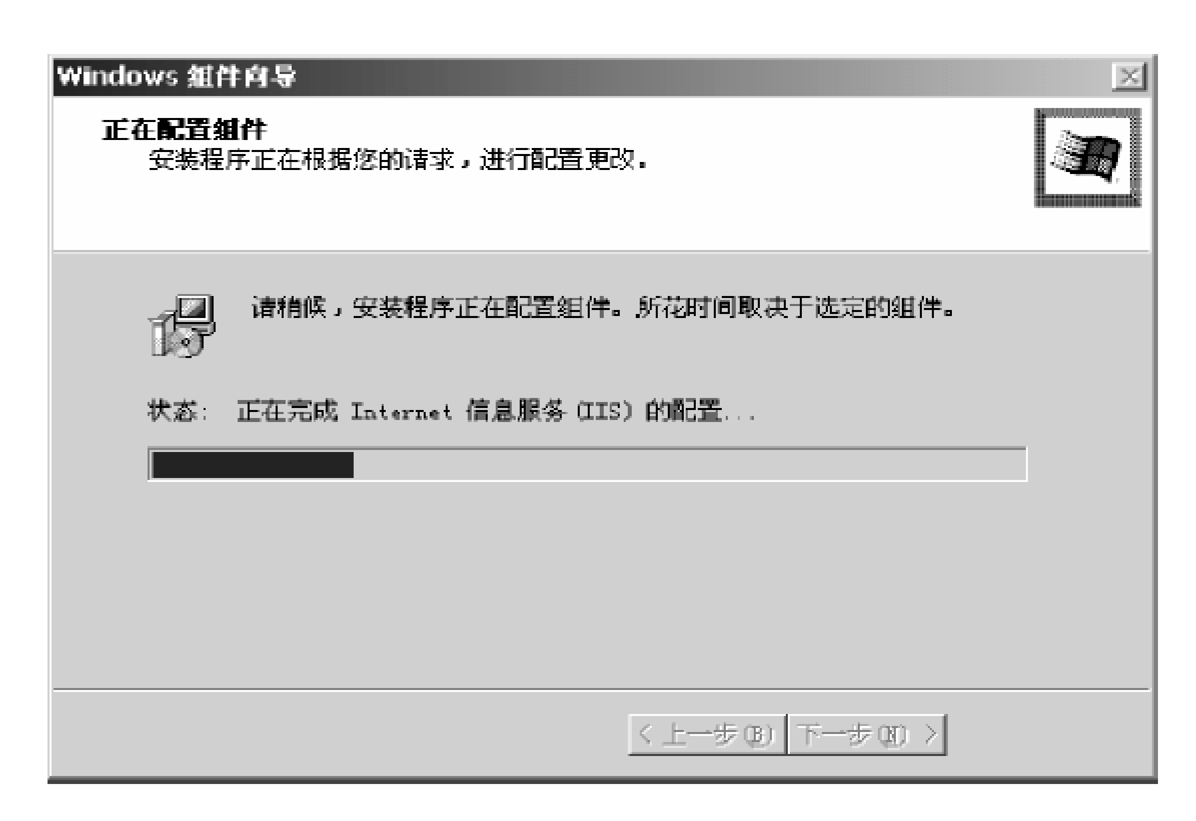


图 4.11 安装进行组件配置



图 4.12 设置站点属性



图 4.13 设置服务器证书

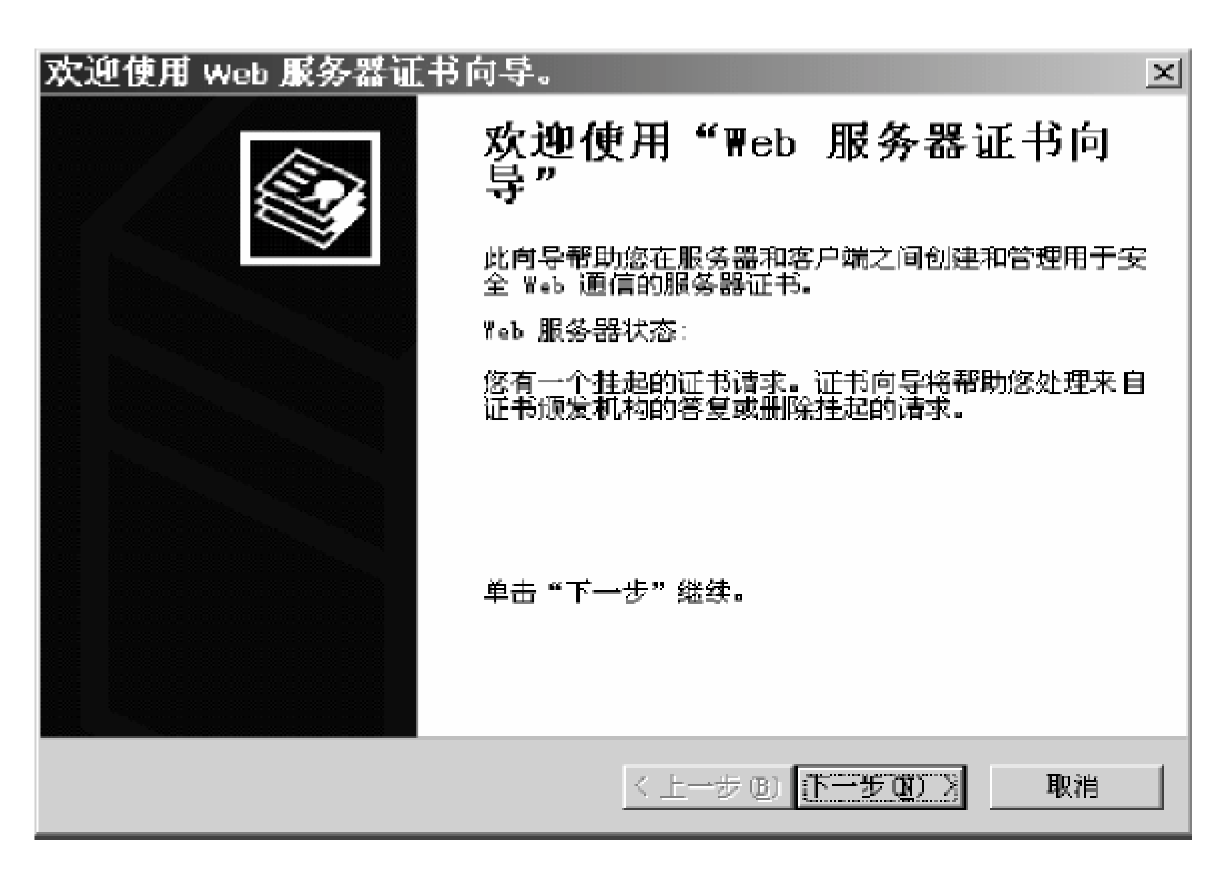


图 4.14　启动服务器证书安装向导

（3）单击“下一步”按钮，选择“创建一个新证书”单选按钮，如图 4.15 所示。

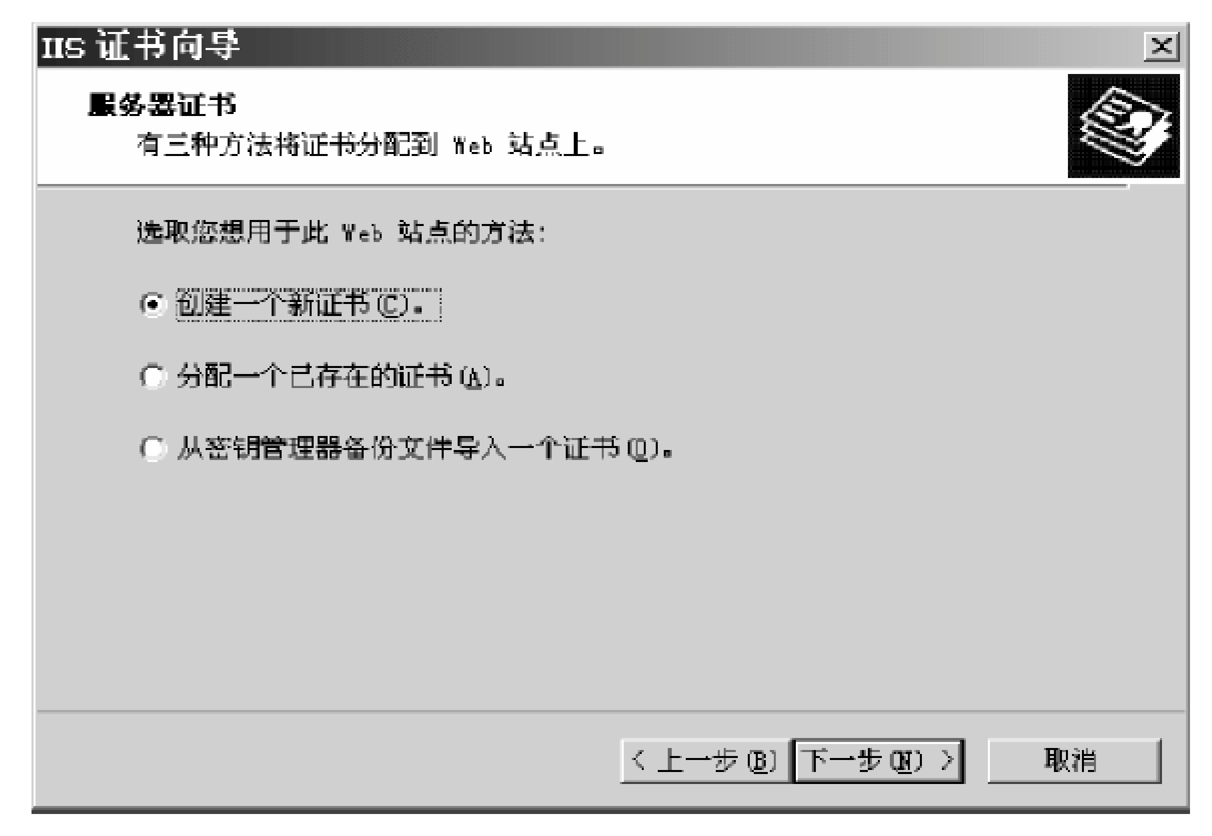


图 4.15　创建新证书

（4）选择“现在准备请求，但稍候发送”单选按钮，如图 4.16 所示。

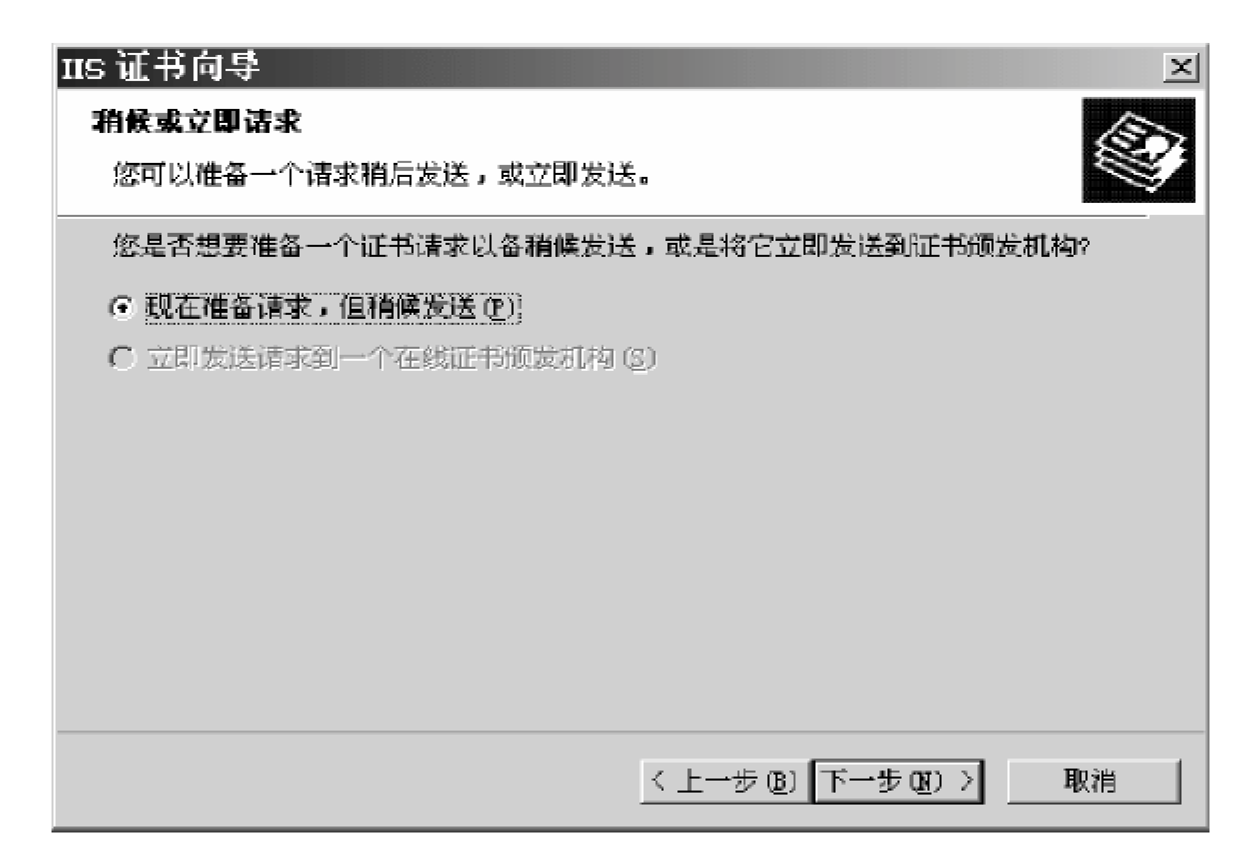


图 4.16　提交证书申请

(5) 为证书设置名称和加密密钥的长度，如图 4.17 所示。

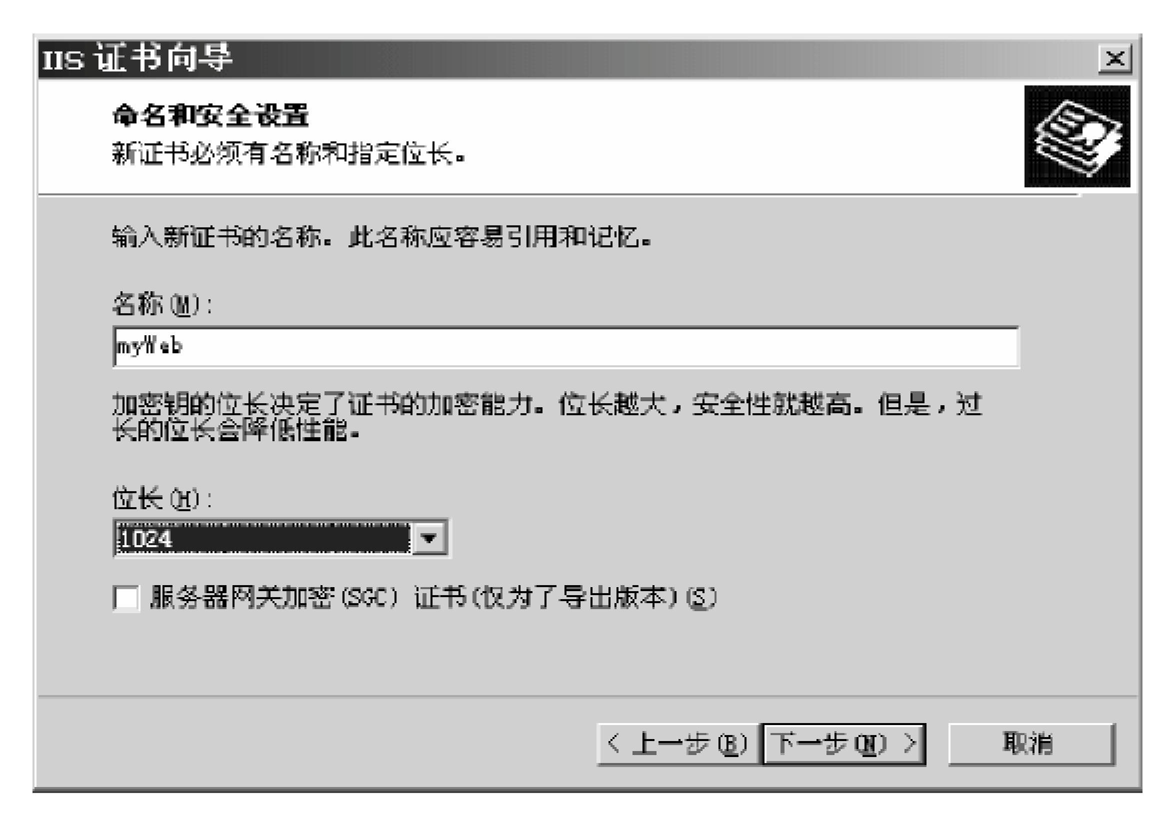


图 4.17　设置证书基本信息(1)

(6) 为证书设置组织名称和部门，如图 4.18 所示。

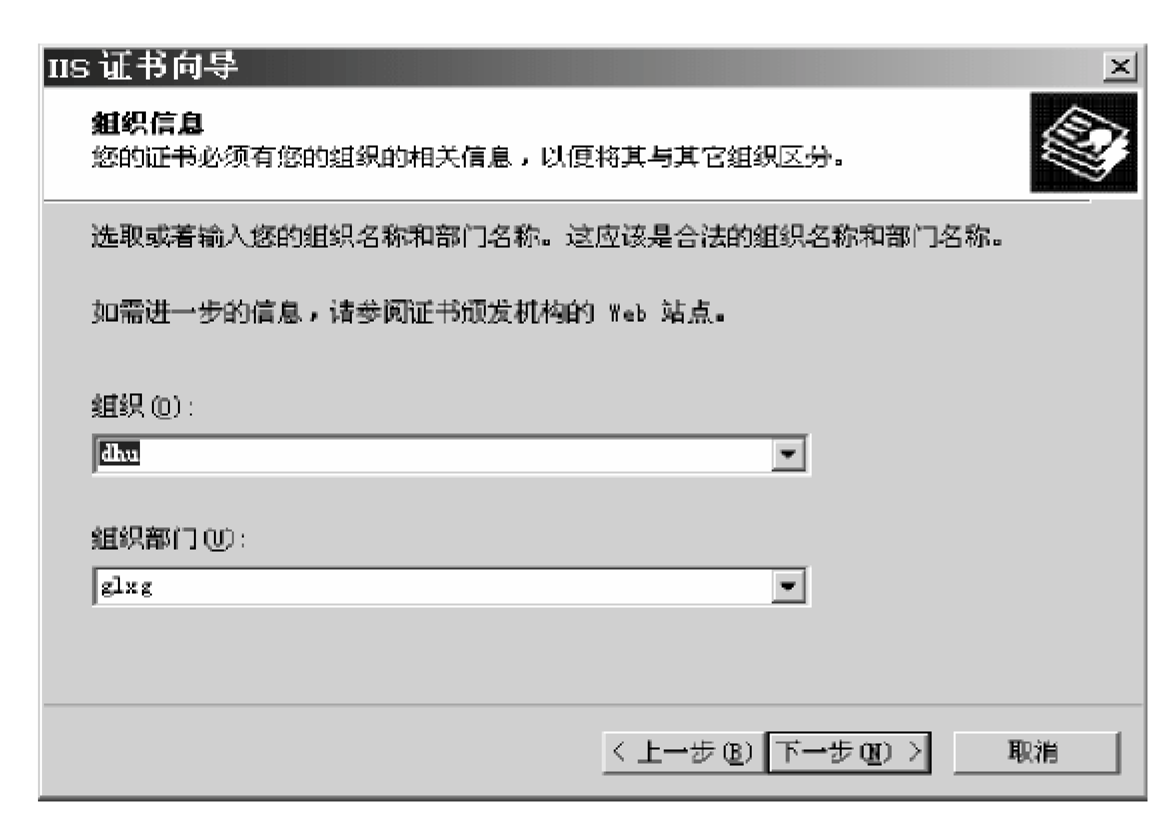


图 4.18　设置证书基本信息(2)

(7) 为证书设置站点公用名称，如图 4.19 所示。

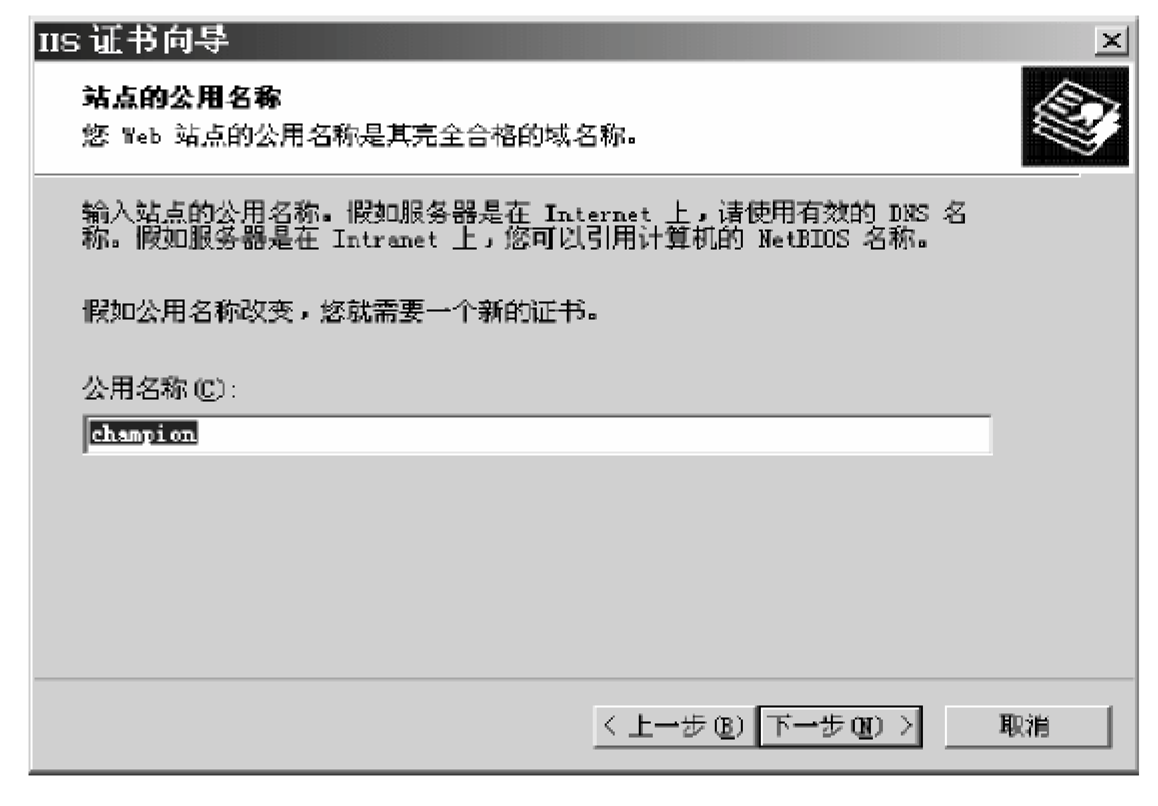


图 4.19　设置证书基本信息(3)

(8)为证书设置颁发机构的地理信息,如图 4.20 所示。

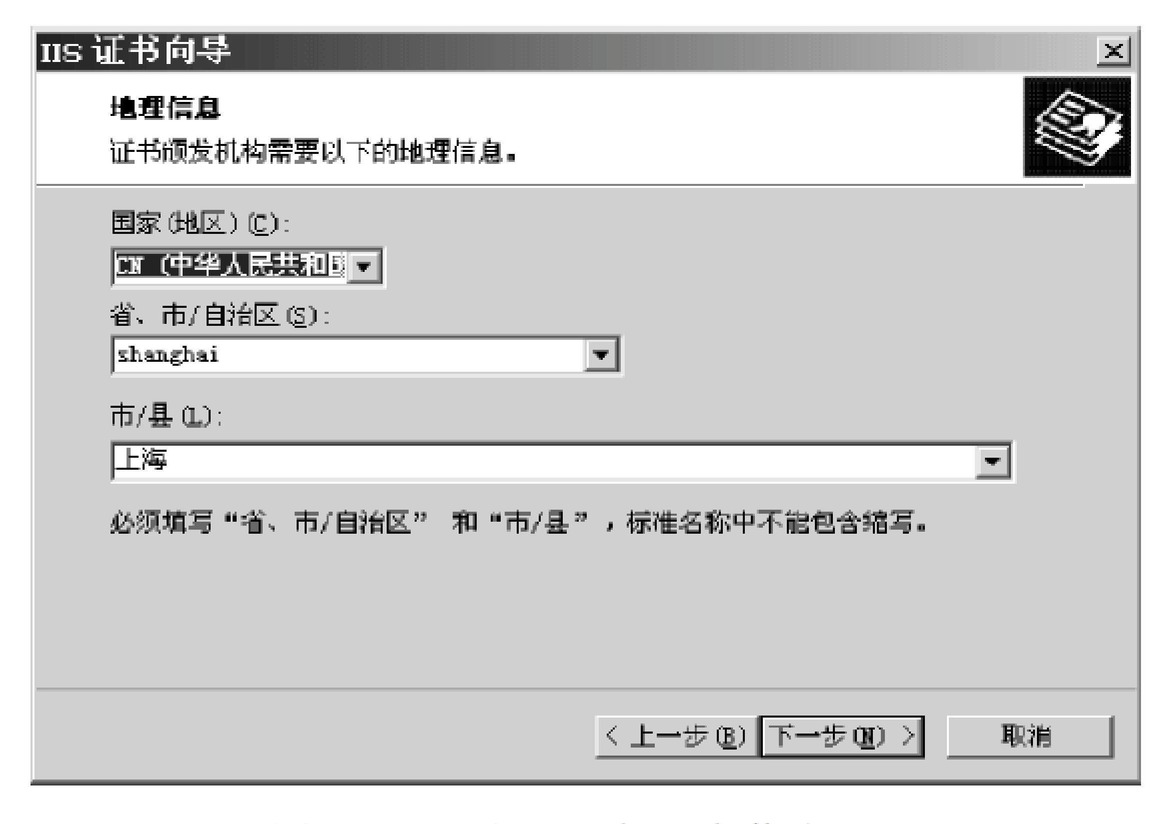


图 4.20 设置证书基本信息(4)

(9)设置证书请求文件名及位置,如图 4.21 所示。

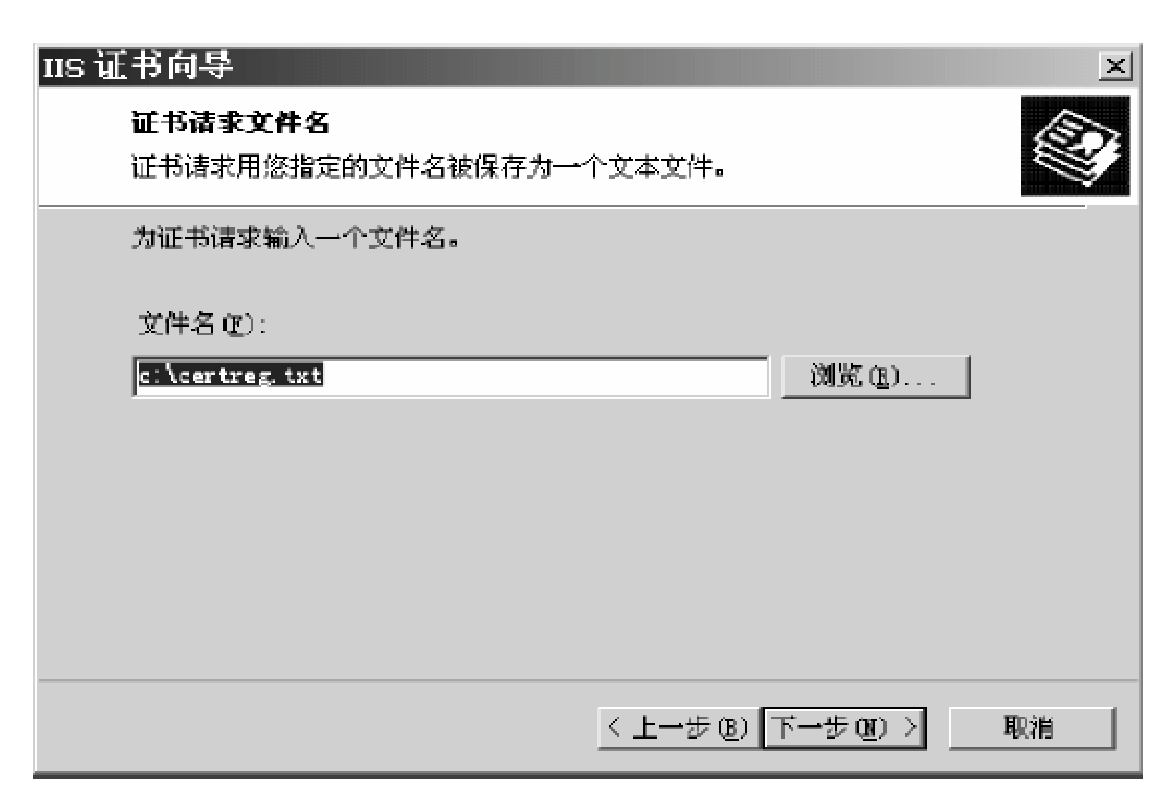


图 4.21 设置证书请求保存文件

(10)单击"下一步"按钮完成证书设置,出现证书请求文件的摘要信息,如图 4.22 所示。



图 4.22 证书请求文件摘要信息

(11) 确认后单击“下一步”按钮完成证书向导,生成 Web 站点的证书请求文件,如图 4.23 所示。

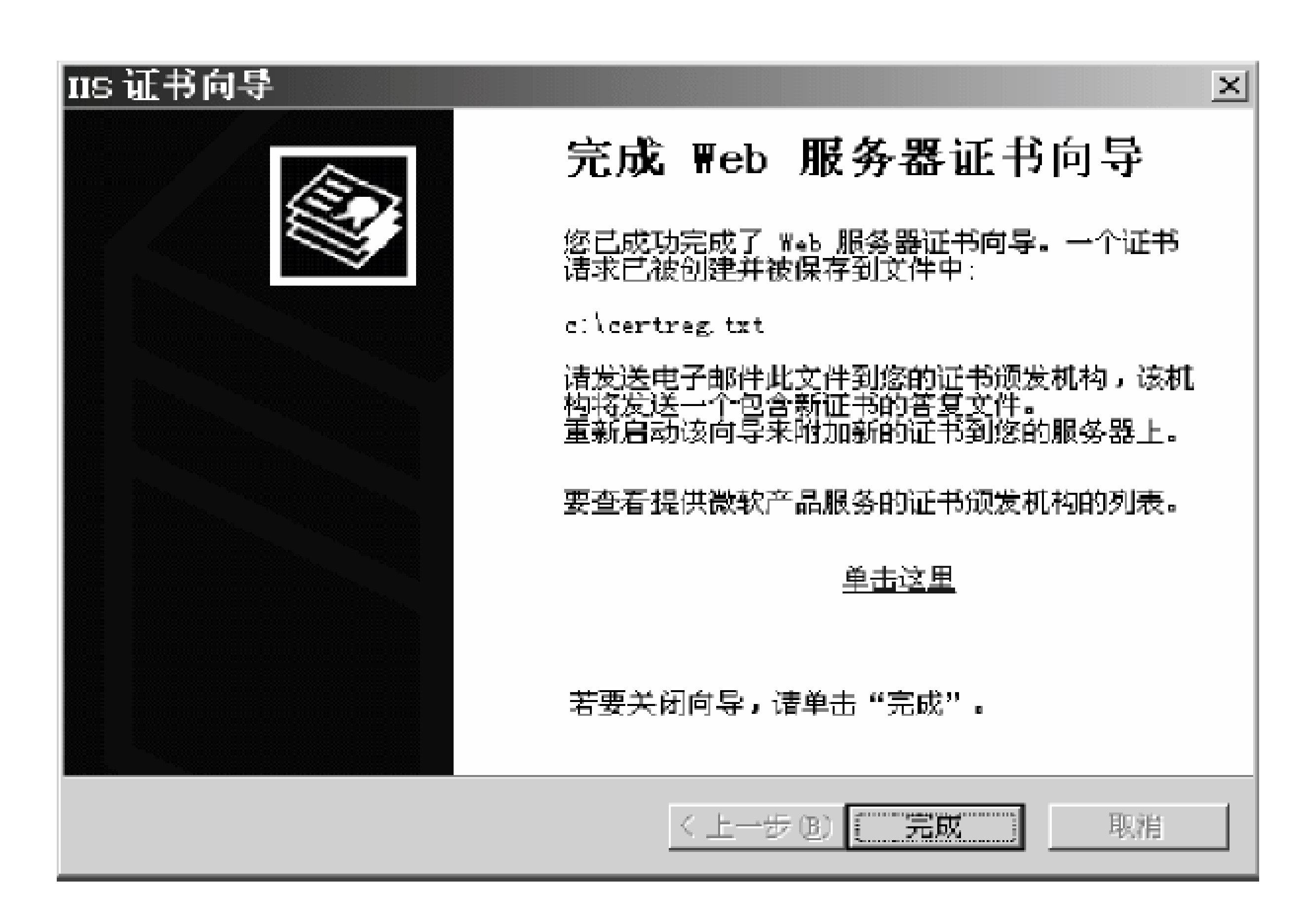


图 4.23　完成服务器证书向导

(12) 打开 IE 浏览器,输入“http://CA IP/certsrv/”,其中 CA IP 为证书颁发机构服务器 IP 地址,提交网站证书请求文件,向证书颁发机构申请证书,如图 4.24 所示,选择“申请证书”单选按钮。

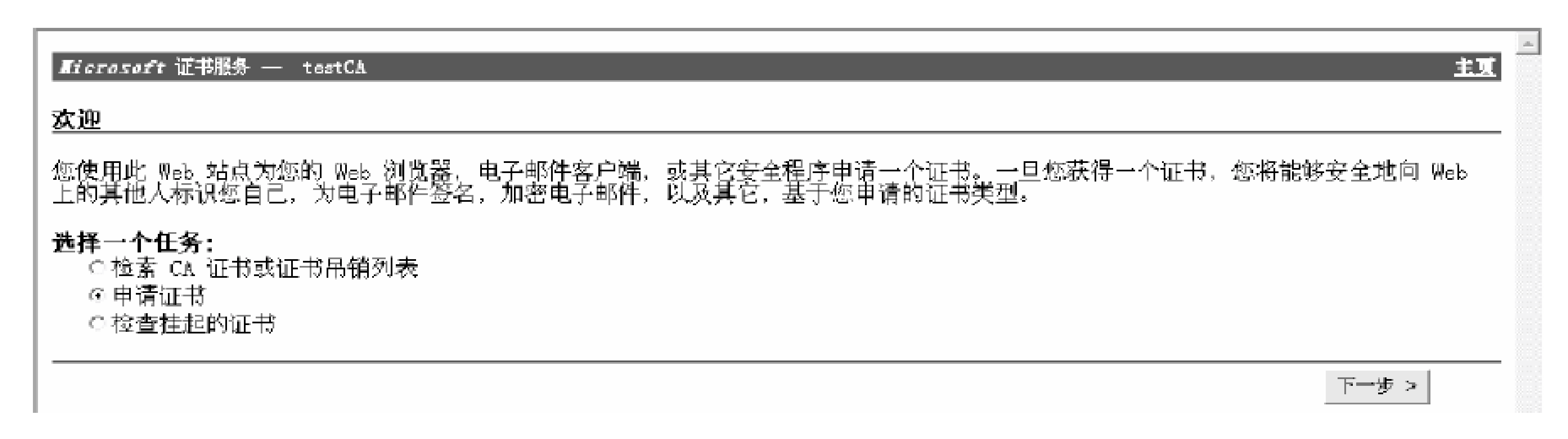


图 4.24　向证书颁发机构申请证书

(13) 选择“高级申请”单选按钮,单击“下一步”按钮,如图 4.25 所示。

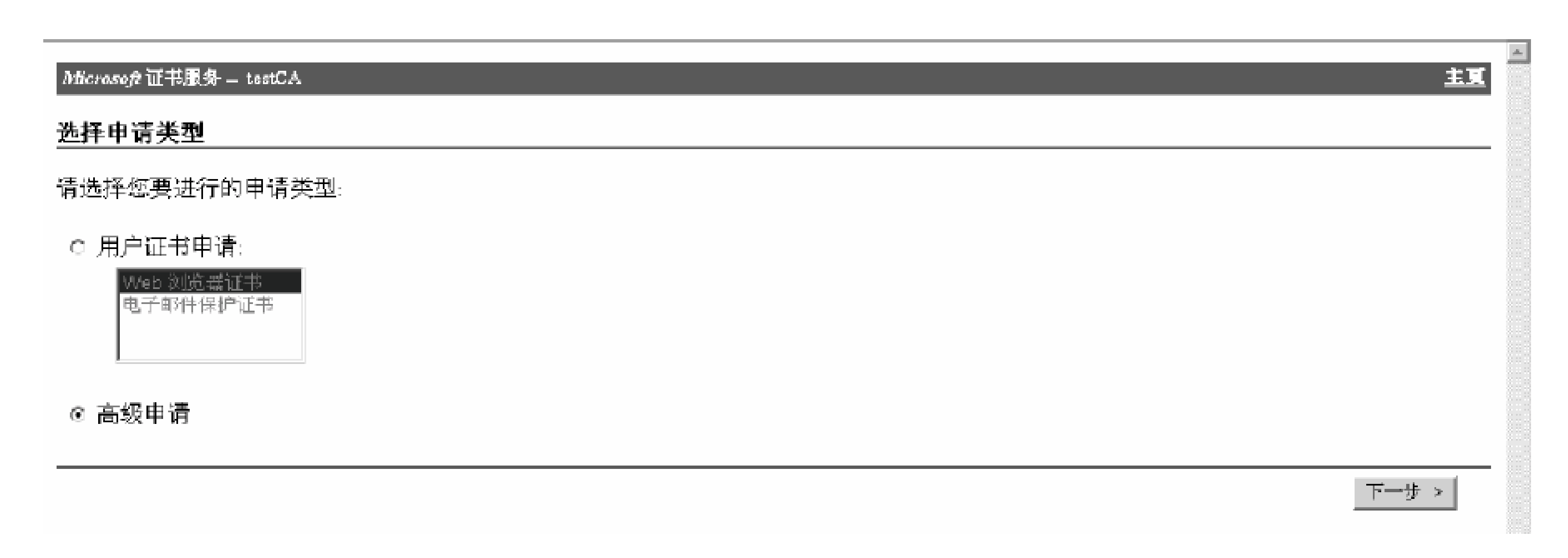


图 4.25　选择申请类型

（14）在高级证书申请中，选择“使用 base64 编码的 PKCS ＃10 文件提交一个证书申请，或使用 base64 编码的 PKCS ＃7 文件更新证书申请。”单选按钮，如图 4.26 所示。

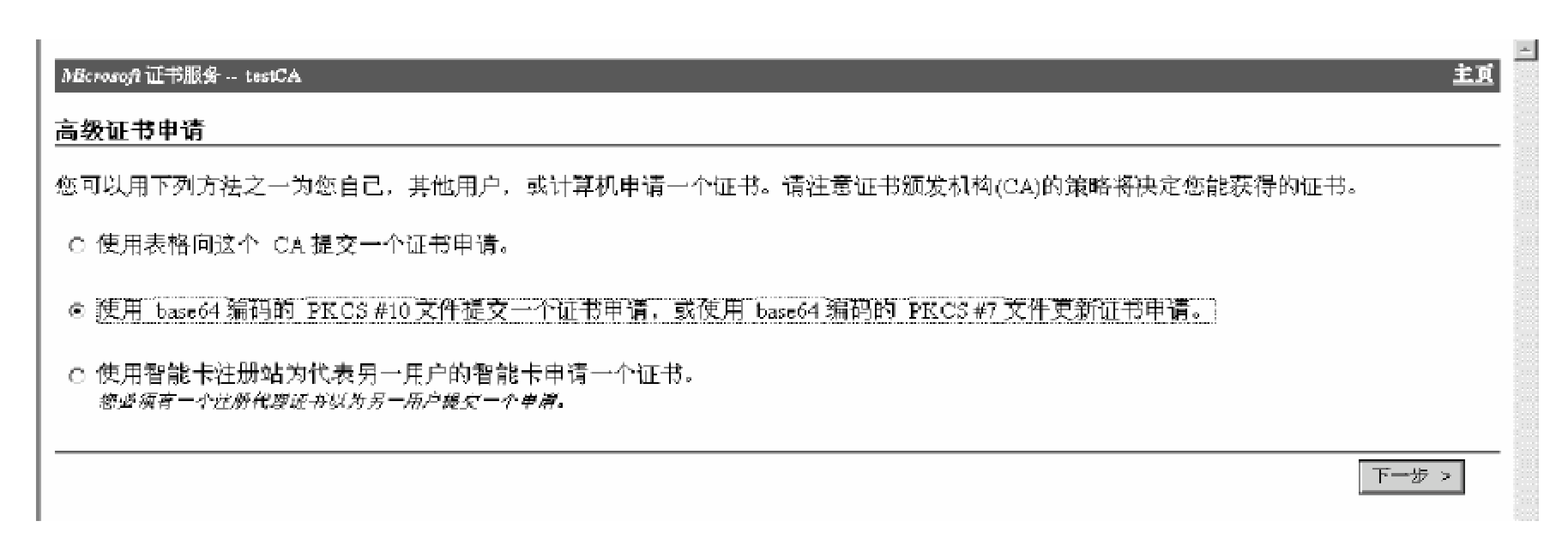


图 4.26　选择证书申请方式

（15）打开上面操作中存放的证书请求文件 certreq.txt，将其内容复制到“保存的申请”文本框内进行提交，如图 4.27 所示。



图 4.27　提交保存的证书

（16）证书被挂起，等待证书颁发机构的审批，如图 4.28 所示。

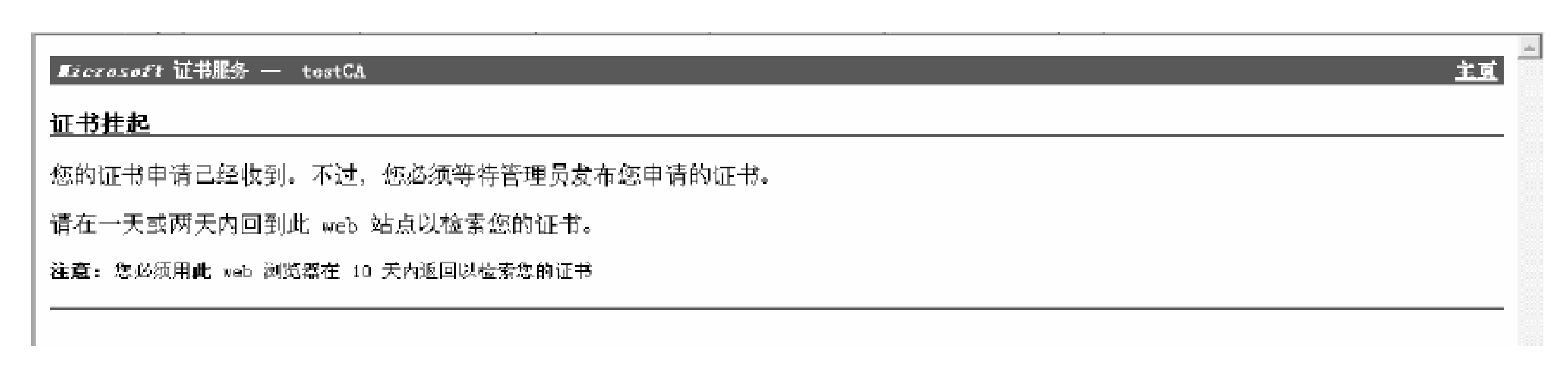


图 4.28　证书被挂起

3）CA 机构颁发证书

（1）在“开始”|“程序”|“管理工具”中选择“证书颁发机构”，打开相应的管理窗口，如图 4.29 所示。

（2）选择“待定申请”，在窗口右边将列出已提出申请但未回复的证书申请，如图 4.30 所示。



图 4.29　证书颁发机构审核证书(1)

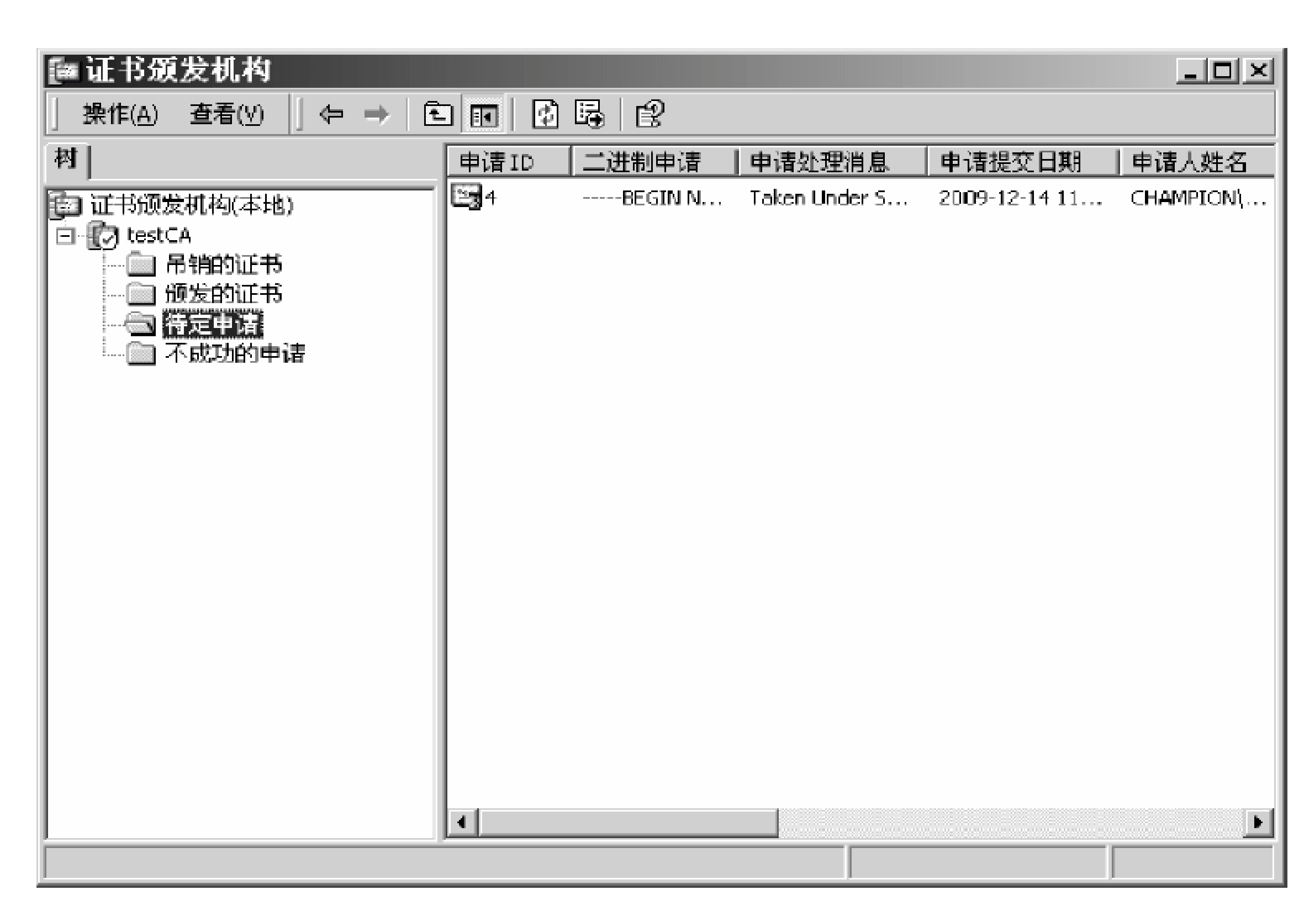


图 4.30　证书颁发机构审核证书(2)

(3) 选中一个待定申请，右击，在弹出的快捷菜单中选择“所有任务”|“颁发”，如图 4.31 所示。



图 4.31　证书颁发机构颁发证书

(4) 选择窗口左边的“颁发的证书”,会看到刚刚颁发的证书,如图 4.32 所示。

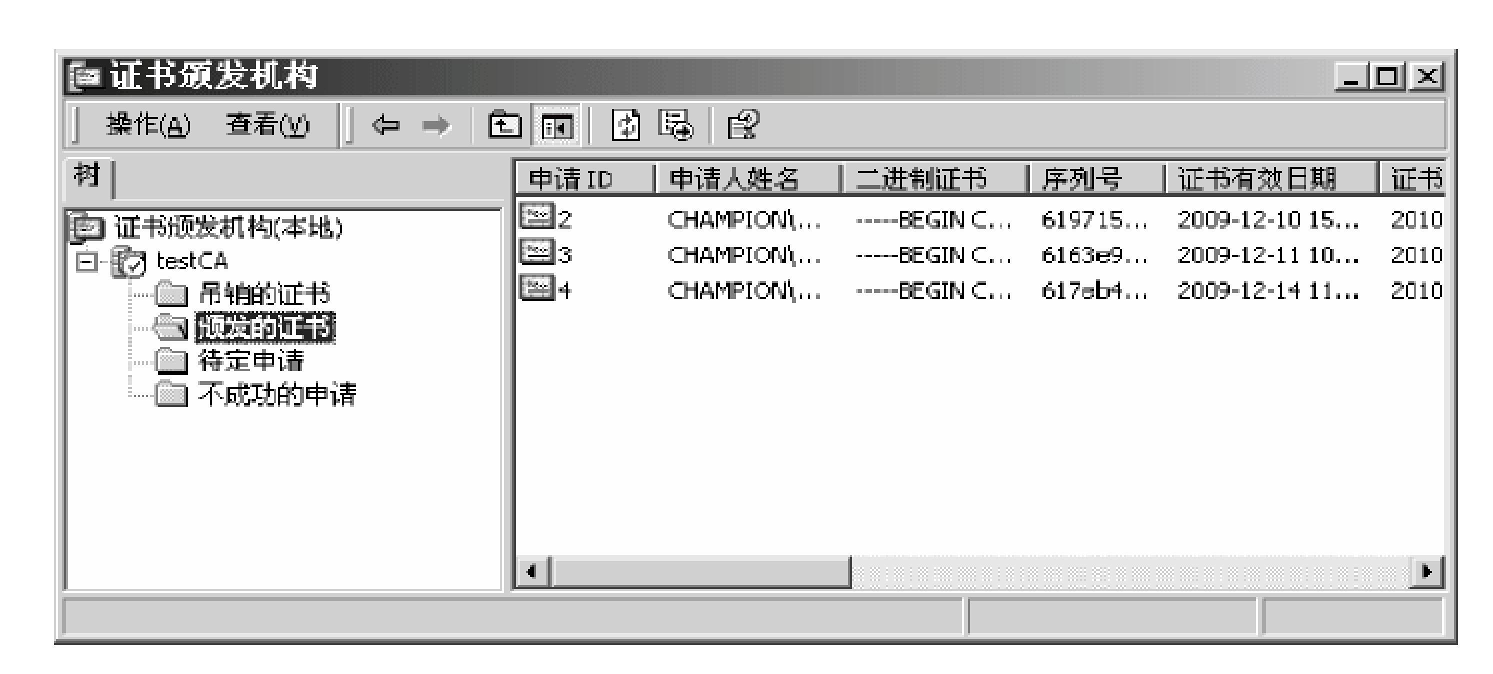


图 4.32 查看已颁发的证书

4) Web 网站下载、安装 CA 颁发的证书

(1) 打开 IE 浏览器,输入“http://CA IP/certsrv/”,其中 CA IP 为证书颁发机构服务器 IP 地址,选择“检查挂起的证书”单选按钮,如图 4.33 所示。

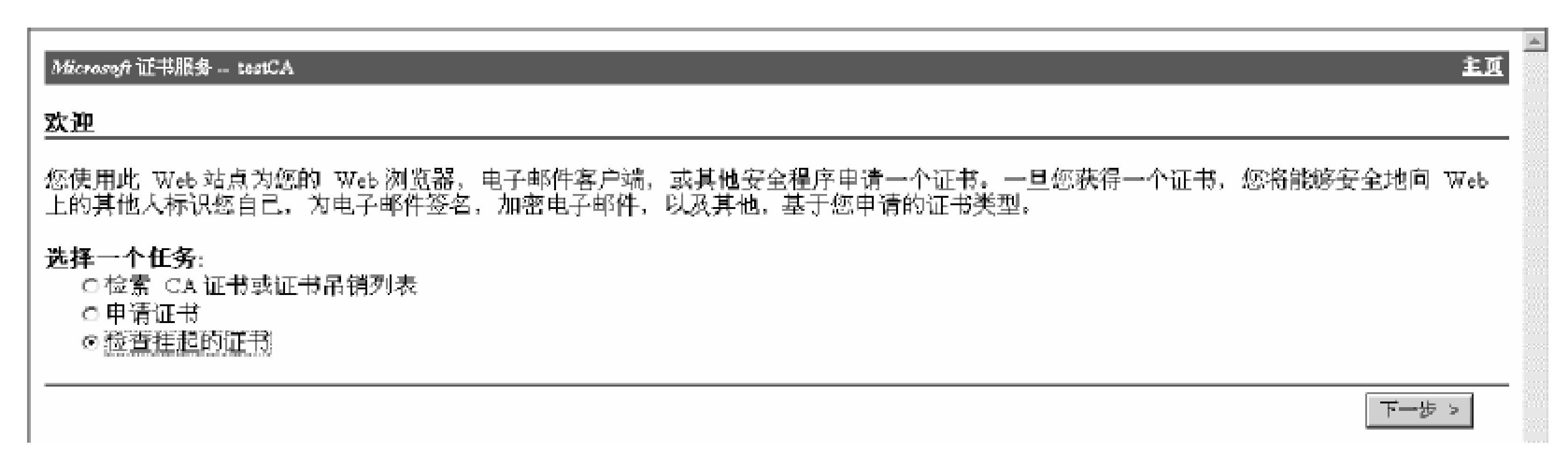


图 4.33 下载 CA 颁发的证书

(2) 选择已申请的证书,如图 4.34 所示。

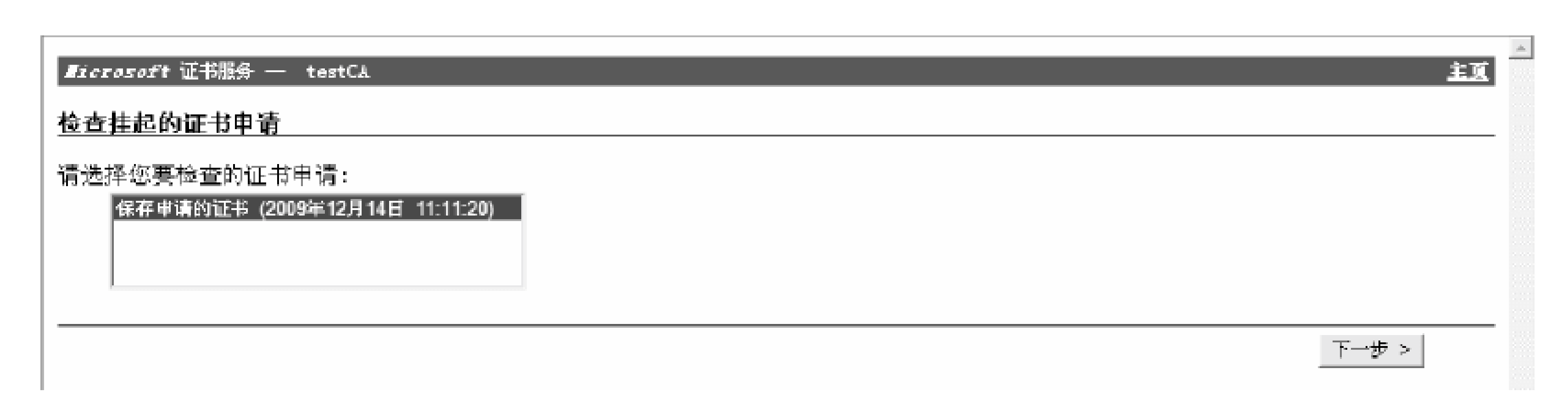


图 4.34 选择查看的证书申请

(3) 在弹出的窗口中单击“下载 CA 证书”链接,如图 4.35 所示。

(4) 保存证书并确定保存路径和文件名,如图 4.36 和图 4.37 所示。

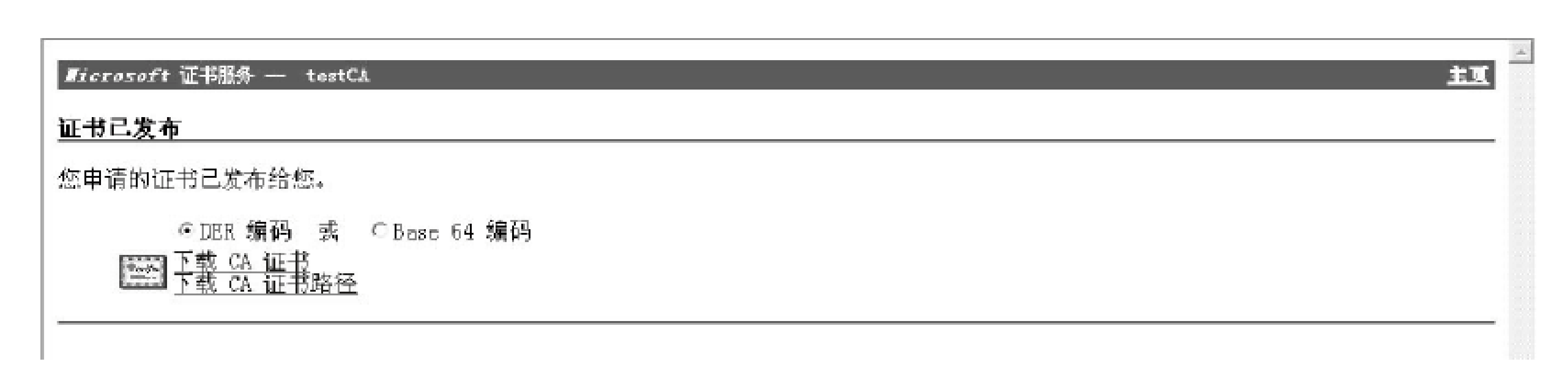


图 4.35 下载 CA 证书

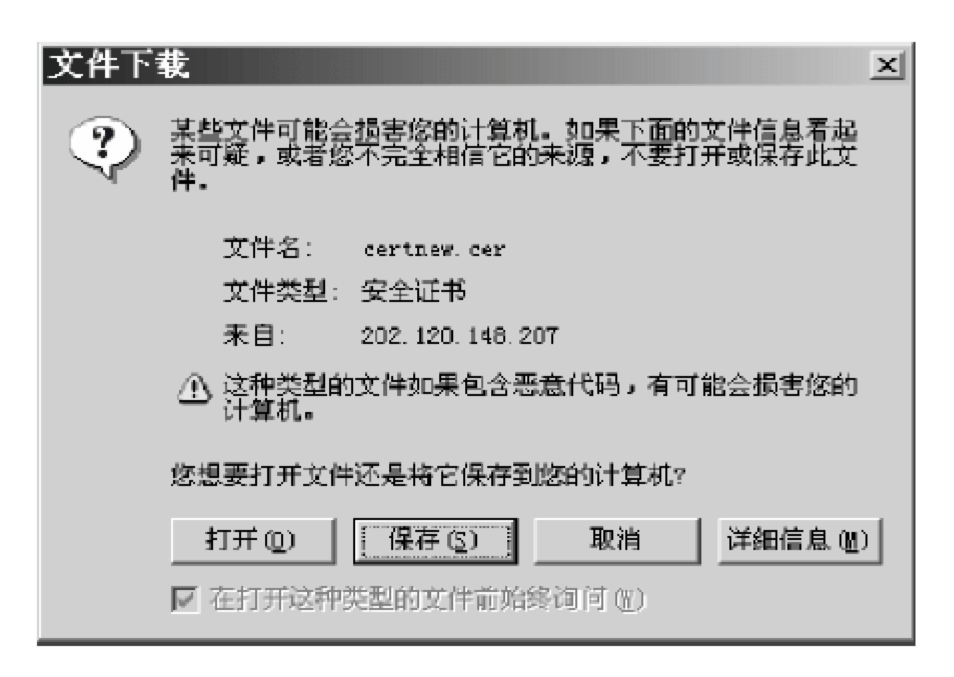


图 4.36　下载证书



图 4.37　保存证书

(5) 选择“开始”|“程序”|“管理工具”|“Internet 服务管理器”命令，打开相应窗口，选中默认 Web 站点，右击，在弹出的快捷菜单中选择“属性”，在打开的属性对话框中单击“目录安全性”选项卡，如图 4.38 所示。

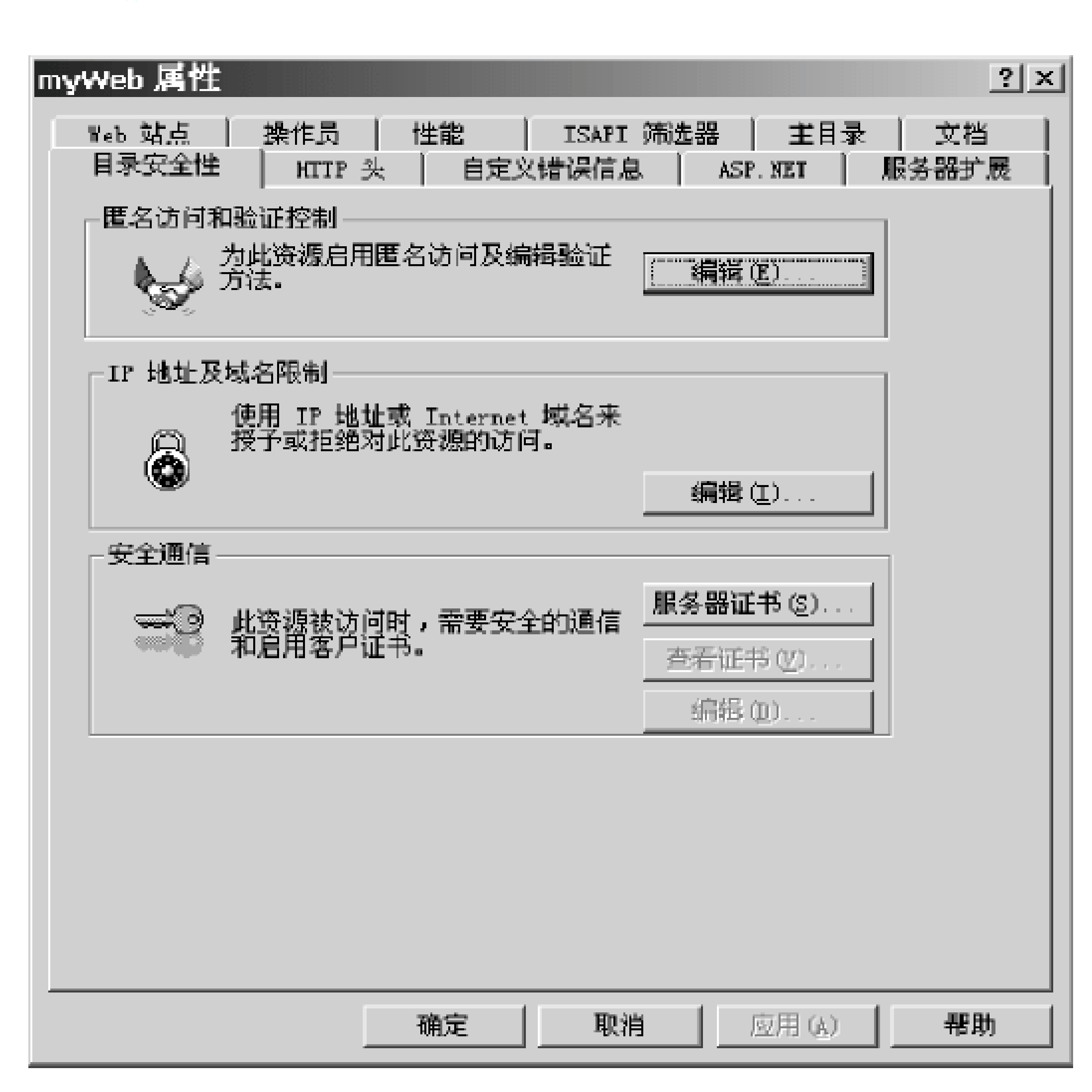


图 4.38　打开站点属性对话框

(6) 单击“服务器证书”按钮，启动证书向导，选择“处理挂起的请求并安装证书”单选按钮，如图 4.39 所示。

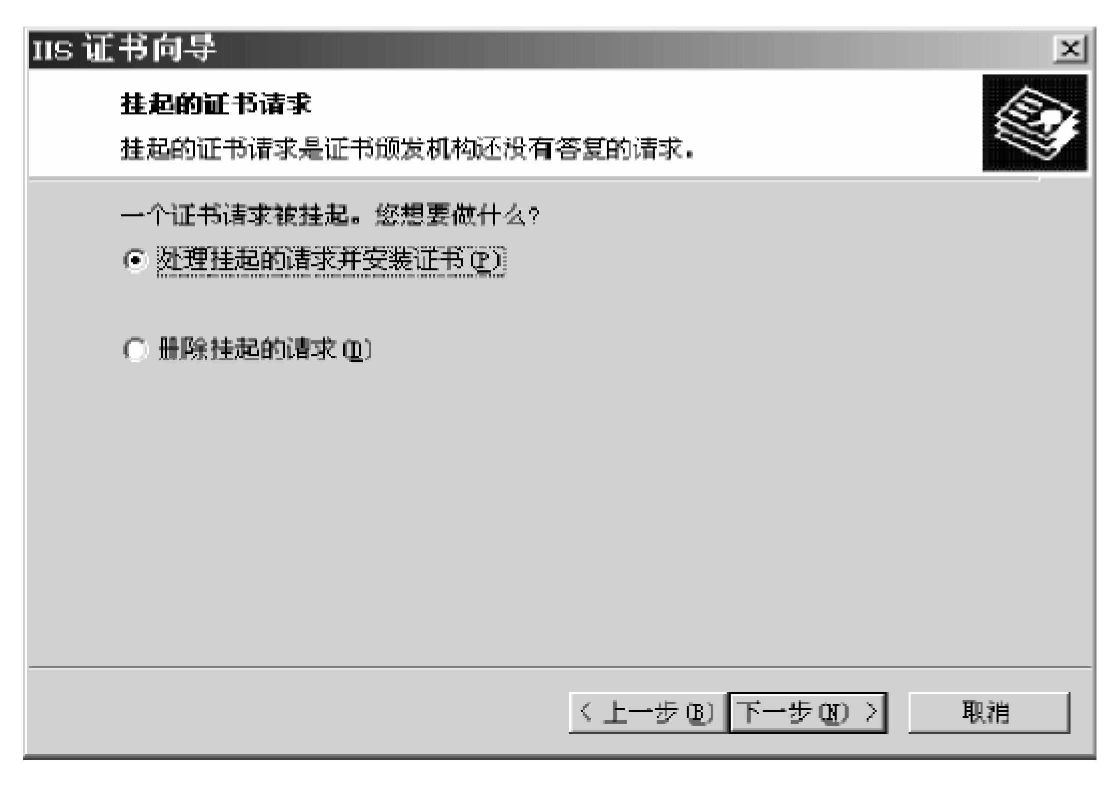


图 4.39　处理挂起的证书请求

(7) 选择刚刚存放证书的路径和文件名，如图 4.40 所示。

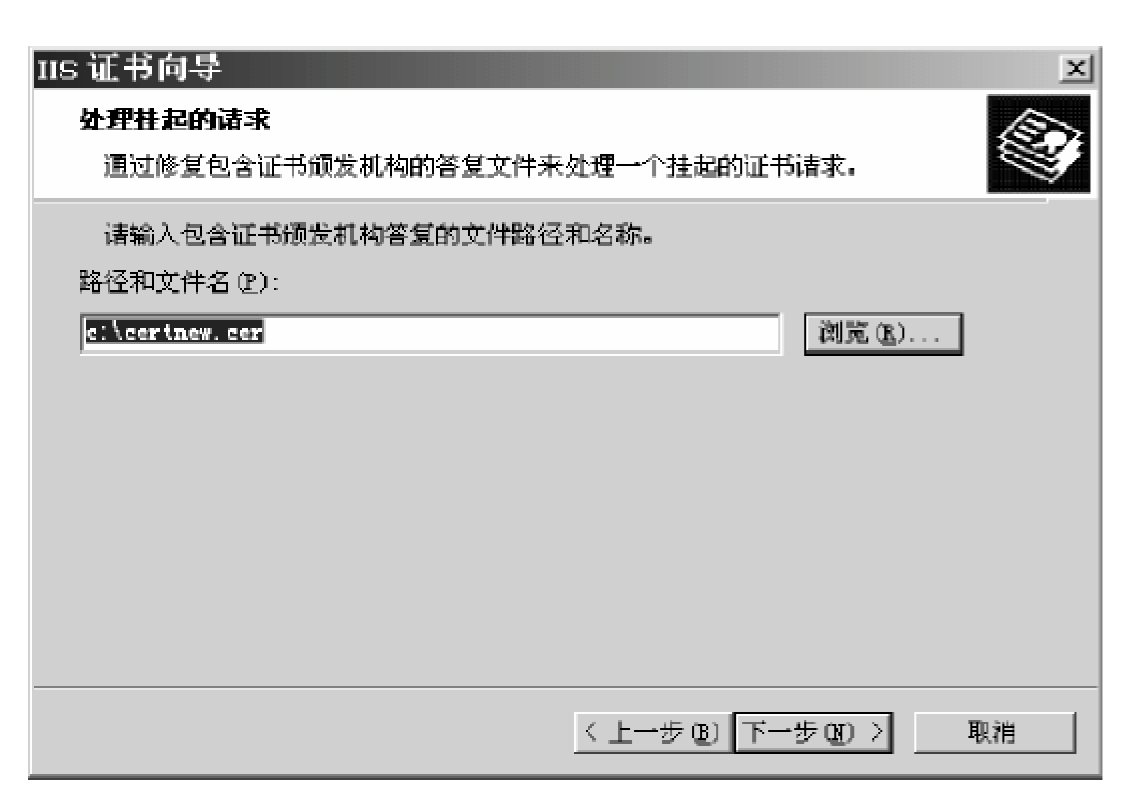


图 4.40　选择所保存的证书文件

(8) 显示证书摘要信息并完成证书的安装，如图 4.41 所示。



图 4.41　安装证书

(9) 在 Web 站点属性对话框中，单击“编辑”按钮，如图 4.42 所示。

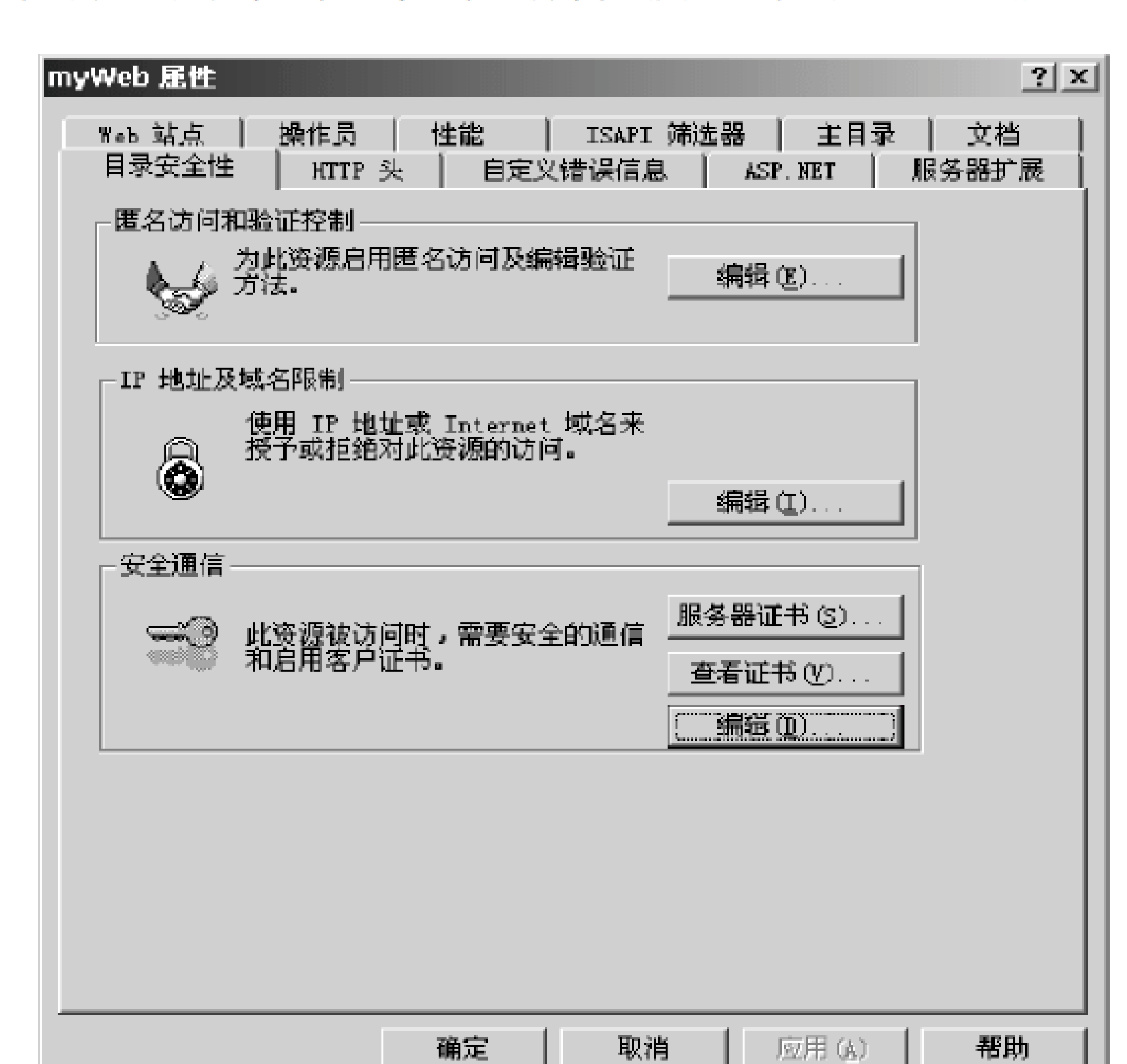


图 4.42　编辑安全通信方式

(10) 在弹出的“安全通信”对话框中，选中“申请安全通道(SSL)”复选框，如图 4.43 所示。

(11) 在 Web 站点属性对话框中，单击“查看证书”按钮，查看刚刚安装的证书的详细信息，如图 4.44 所示。



图 4.43　申请 SSL 安全通道



图 4.44　查看已安装证书信息

(12) 通过 IE 浏览器访问刚刚安装了证书的 Web 网站，可以发现网站要求访问者使用 HTTPS 安全协议来代替原来的 HTTP 协议，如图 4.45 所示。

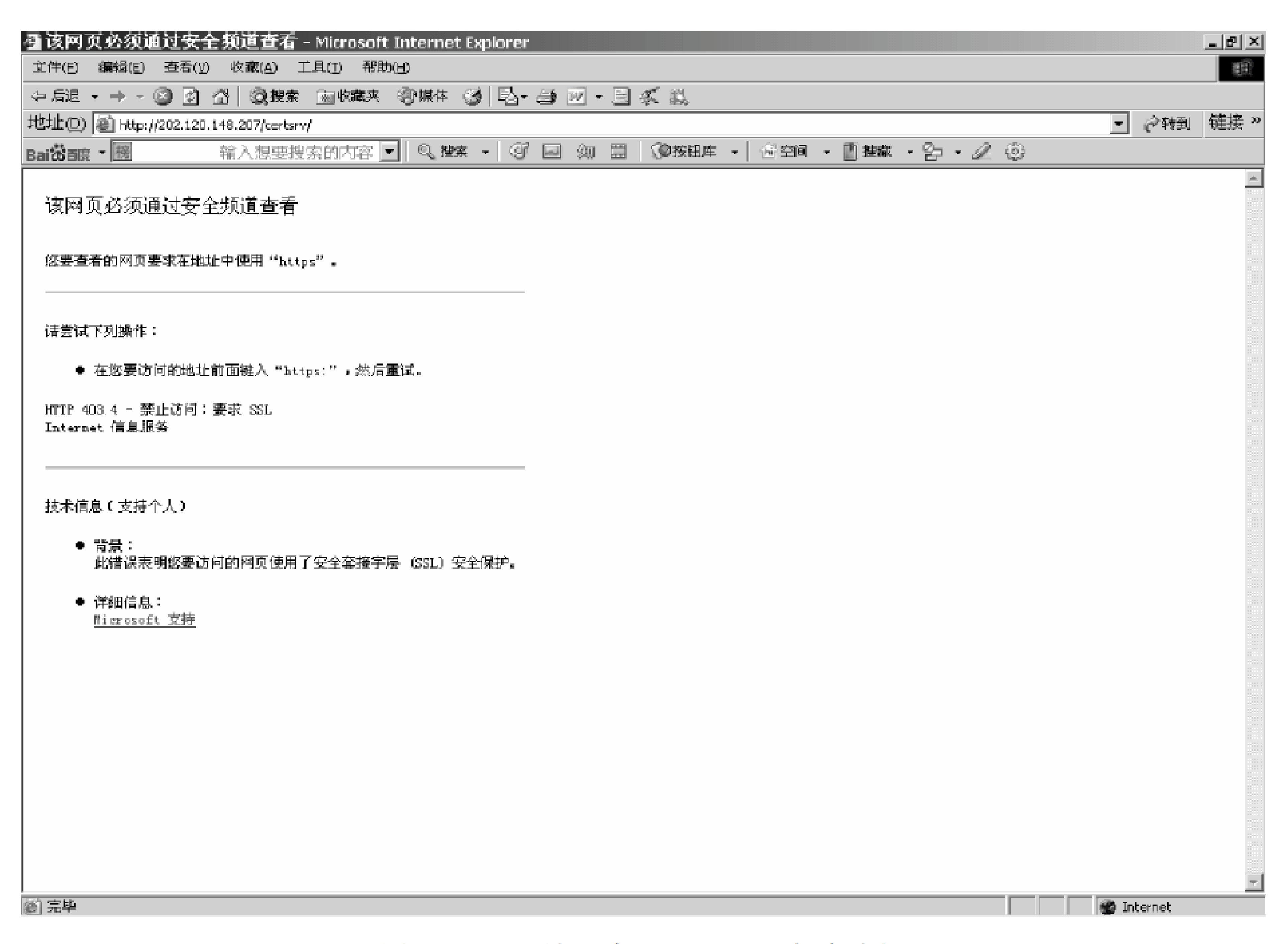


图 4.45　网站要求以 HTTPS 方式访问

(13) 输入"https://CA IP/"，进行网络链接，在弹出的安全警告对话框中单击"确定"按钮，并在后续弹出的警告框中选择"是"，由于相应服务器上没有主页可以显示，将看到如图 4.46 所示内容，可以发现与 Web 网站的 SSL 安全通道已经建立。

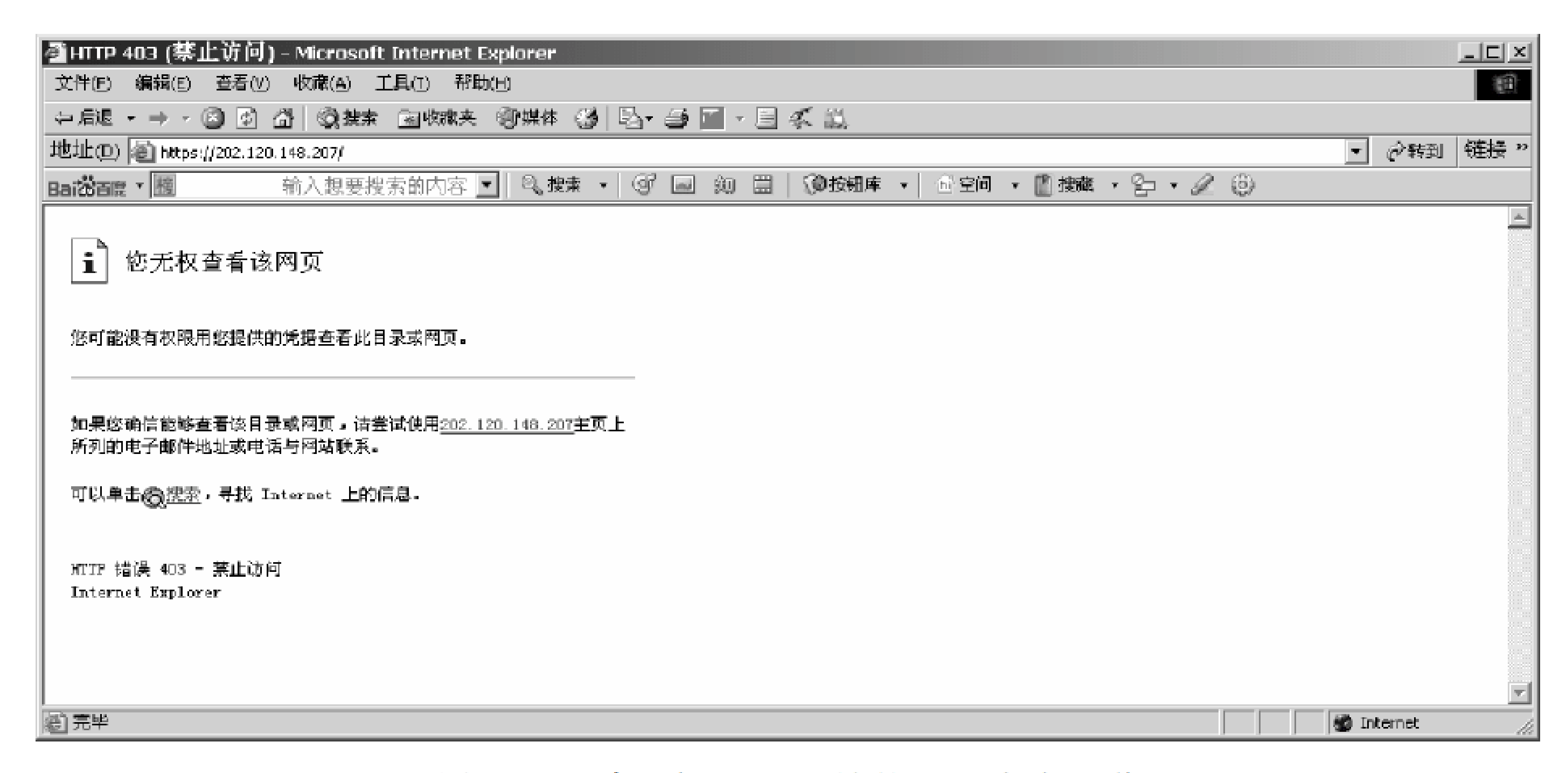


图 4.46　建立与 Web 网站的 SSL 安全通道

6. 实验报告与要求

根据上面介绍的各项实验要求，详细观察记录证书服务和 Web 网站 SSL 安全通信开

通前后系统的变化，给出分析报告。

7. 实验分析与讨论

在SSL通信中，为了实现更加全面的安全性，可以同时进行客户端身份认证。用户可以参照服务器端证书的申请和安装方法，考虑如何进行客户端证书的申请和安装，并对基于通信双方身份认证的SSL连接启用过程和通信原理进行思考。

8. 注意事项

安装证书服务时，只有域控制器才能安装企业根CA和企业从属CA。

4.2.3　数字证书的申请与使用

1. 实验目的

了解国内外主要的CA机构及其提供的服务种类，掌握数字证书的申请、安装及使用方法。

2. 实验原理

目前国内外各主要CA中心都提供了各种数字证书的相关服务，本实验以天威诚信网上试用型电子邮件数字证书为例介绍了数字证书的申请和使用方法。

3. 实验环境

安装了Windows 2000/XP操作系统的主机一台，配置有Internet Explorer和Outlook Express软件。

4. 实验内容

(1) 通过浏览各数字认证中心网址，了解比较各CA的特点；
(2) 从一家CA中心申请一份数字证书，进行安装；
(3) 对该证书分别进行密钥对和单独公钥的导出保存；
(4) 利用Outlook发送带有数字签名的电子邮件；
(5) 发送加密的电子邮件。

5. 实验步骤

1) 上网浏览各CA中心网址，了解各CA的特点并进行比较，部分CA网址如表4.1所示。

表4.1　部分CA网址

CA名称	网址	CA名称	网址
verisign	www.verisign.com	上海CA	www.sheca.com
北京CA	www.bjca.org.cn	天威诚信	www.itrus.com.cn
广东CA	www.cnca.net	中国金融认证中心	www.cfca.com.cn

2）数字证书的申请与安装

（1）登录到 http://www.itrus.com.cn/Services.php，选择“安全电子邮件服务”试用链接，如图 4.47 所示。

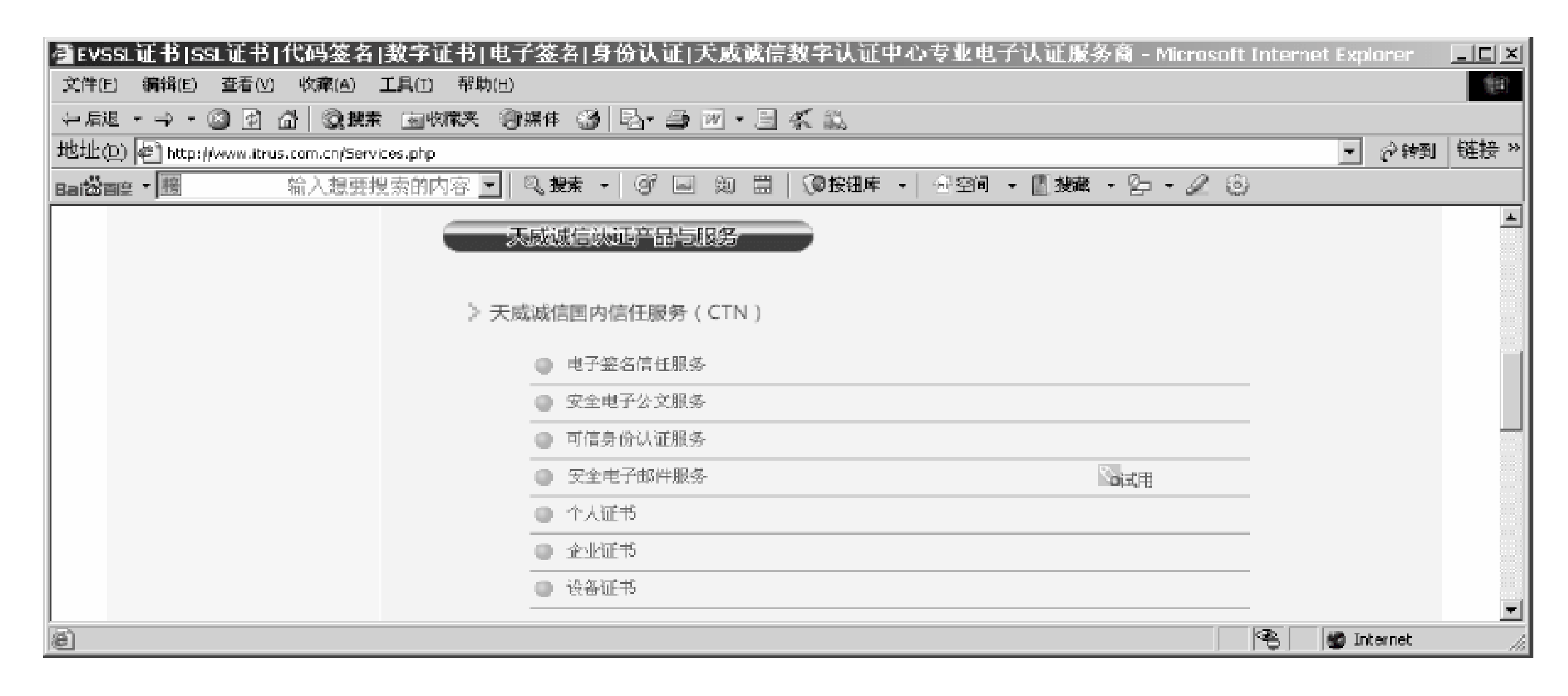


图 4.47　天威诚信证书服务界面

（2）在 https://ica-enroll.itrus.com.cn/cscfree/页面中单击“申请用户证书”链接，如图 4.48 所示。



图 4.48　申请用户证书

（3）进入“用户基本信息”表单，按照表单的提示内容，完整地输入个人资料，单击“确认”按钮，系统将完成数字证书的签发和相关证书链的安装，如图 4.49 和图 4.50 所示。



图 4.49　填写个人资料



图 4.50　下载和安装数字证书

3）查看数字证书及导出保存

（1）首先打开 Internet Explorer，在其菜单栏上选择“工具”|“Internet 选项”命令，在

“Internet 选项”对话框中，选择“内容”选项卡，单击“证书”按钮查看当前信任的证书列表，如图 4.51 所示。



图 4.51 查看证书列表

（2）在“证书”对话框中，打开“个人”选项卡，可以查看到已经申请的个人数字证书列表，如图 4.52 所示。打开“受信任的根证书颁发机构”选项卡，可以看到相应的根证书已添加到证书列表中，如图 4.53 所示。



图 4.52 查看已经申请的个人数字证书

（3）选定需要查看的个人数字证书，然后单击“查看”按钮，可以查看相应数字证书的详细信息，如图 4.54 所示。



图 4.53　查看受信任的根证书



图 4.54　查看证书详细信息

（4）选定需要导出的个人数字证书，然后单击“导出”按钮，根据提示选择“是，导出私钥”单选按钮，可以导出密钥对到指定的文件中，如图 4.55～图 4.58 所示。



图 4.55　证书导出向导

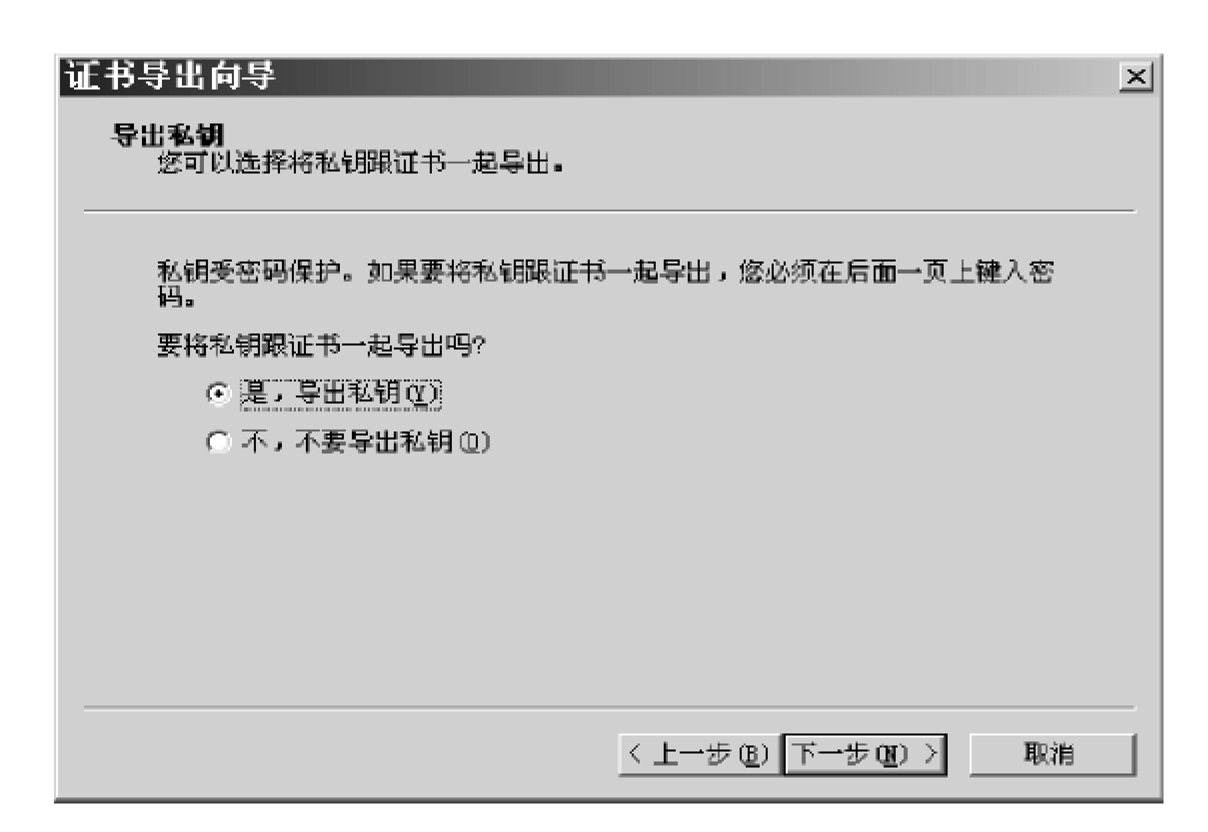


图 4.56　选择导出密钥

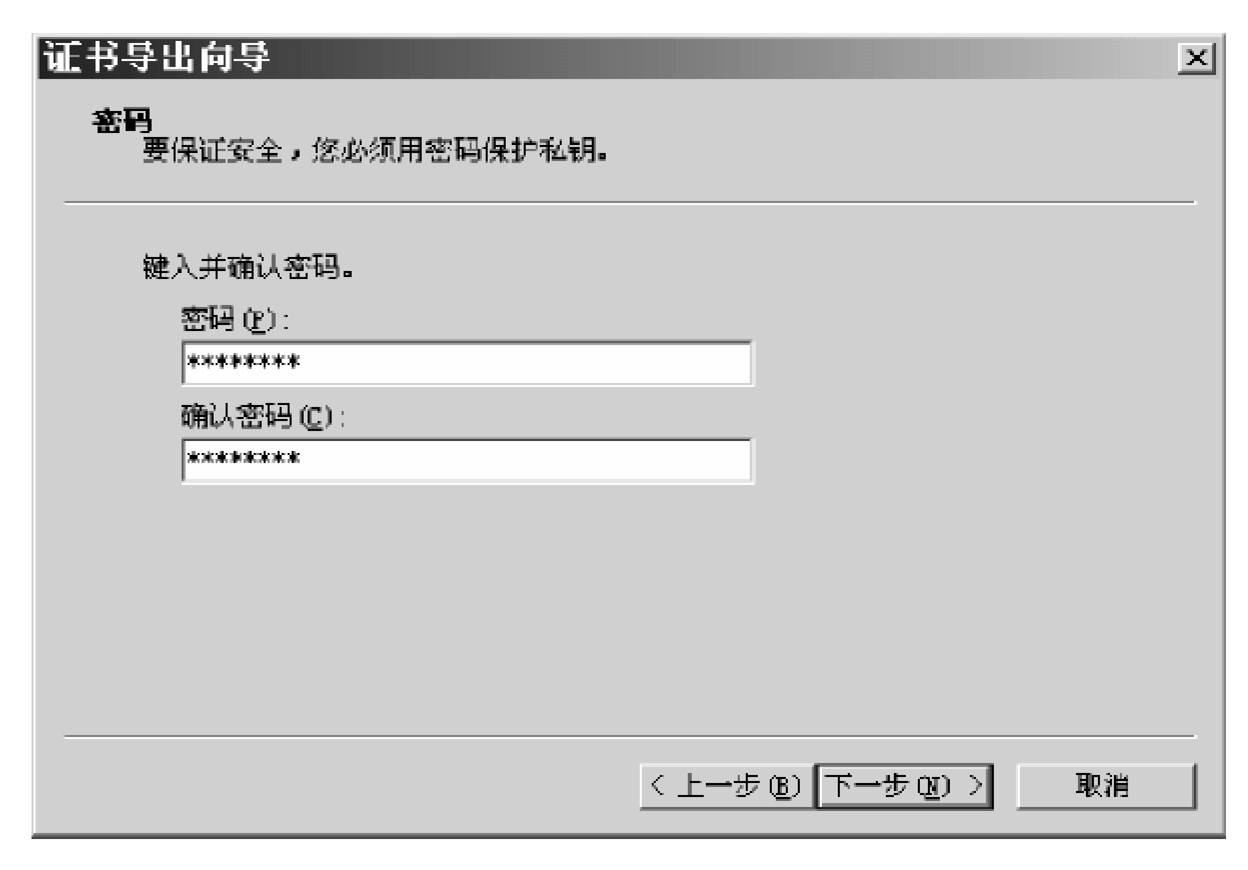


图 4.57　设置私钥保护密码



图 4.58　完成证书导出

(5) 选定需要导出的个人数字证书，然后单击“导出”按钮，根据提示选择“不，不要导出私钥”单选按钮，可以导出公钥对到指定的文件中，如图 4.59 所示。

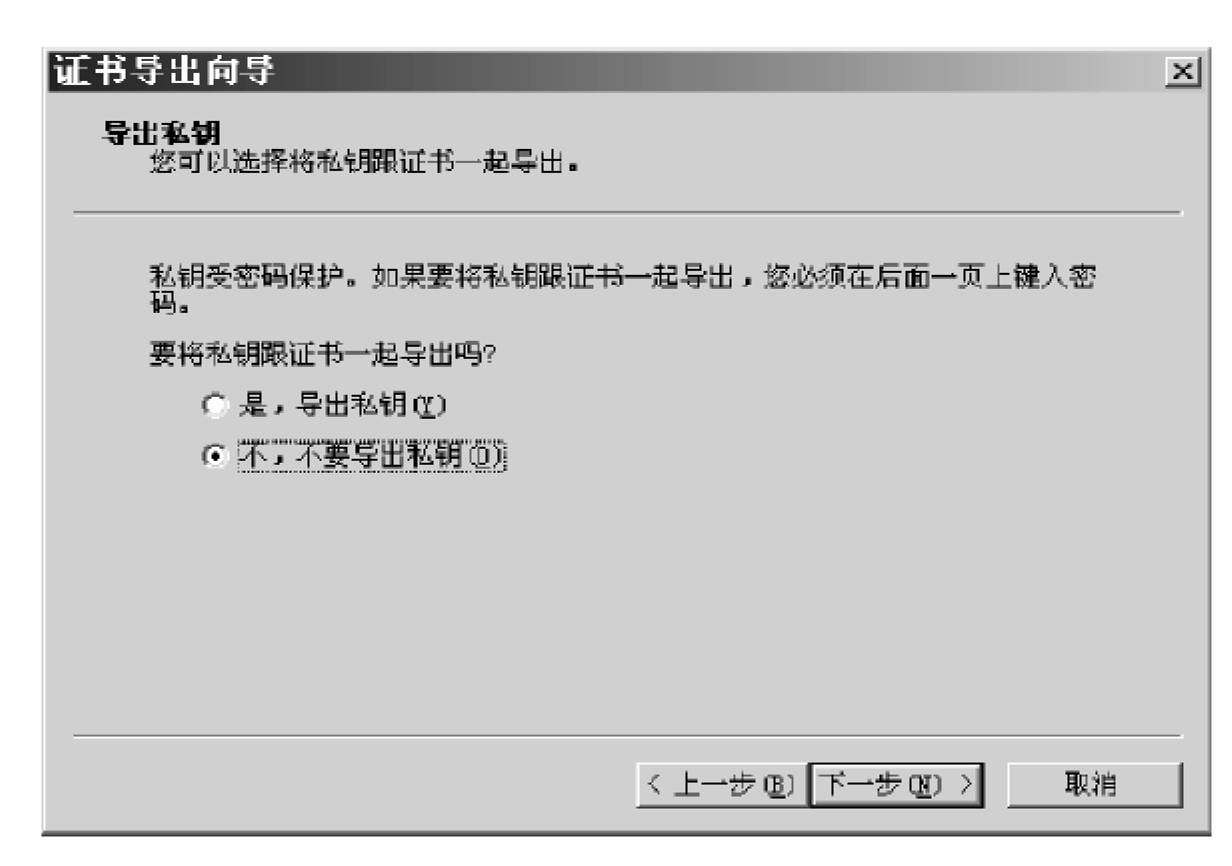


图 4.59　导出公钥

4）使用数字证书发送安全邮件

（1）打开 Outlook Express，选择“工具”|“帐户”命令，在“Internet 帐户”对话框中，单击“添加”按钮，并选择“邮件”选项，进入“Internet 连接向导”对话框，按照系统提示输入相关信息，完成帐号设置，如图 4.60 所示。



图 4.60　Outlook Express 帐号设置

（2）设置邮箱与数字证书绑定：选择“工具”|“帐户”命令，选中“邮件”选项卡中用于发送安全电子邮件的邮件帐户，如图 4.61 所示。然后单击“属性”按钮，进入“属性”对话框。

（3）选择“属性”对话框的“安全”选项卡，可以看到“签署证书”和“加密首选项”这两个选项区域。通过相关设置，可以进行邮件的签署和加密，如图 4.62 所示。



图 4.61　设置邮件帐户属性

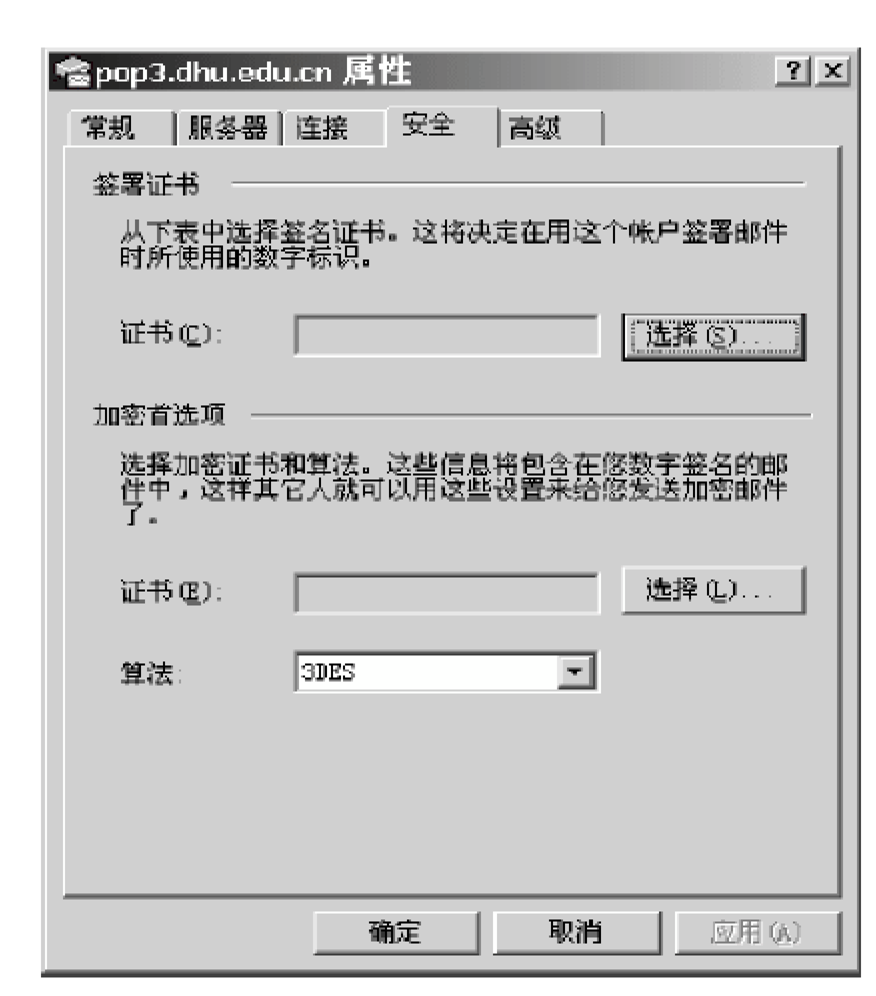


图 4.62　对邮件帐户进行安全设置

（4）单击“签名证书”选项区域中的“选择”按钮，就可以看到自己已经申请的数字证书了。选择自己的数字证书，单击“确定”按钮，即完成了邮箱与证书的绑定，也可以单击“查看

证书”按钮，了解自己的数字证书的详细信息。最后单击“确定”按钮即可，如图 4.63 和图 4.64 所示。

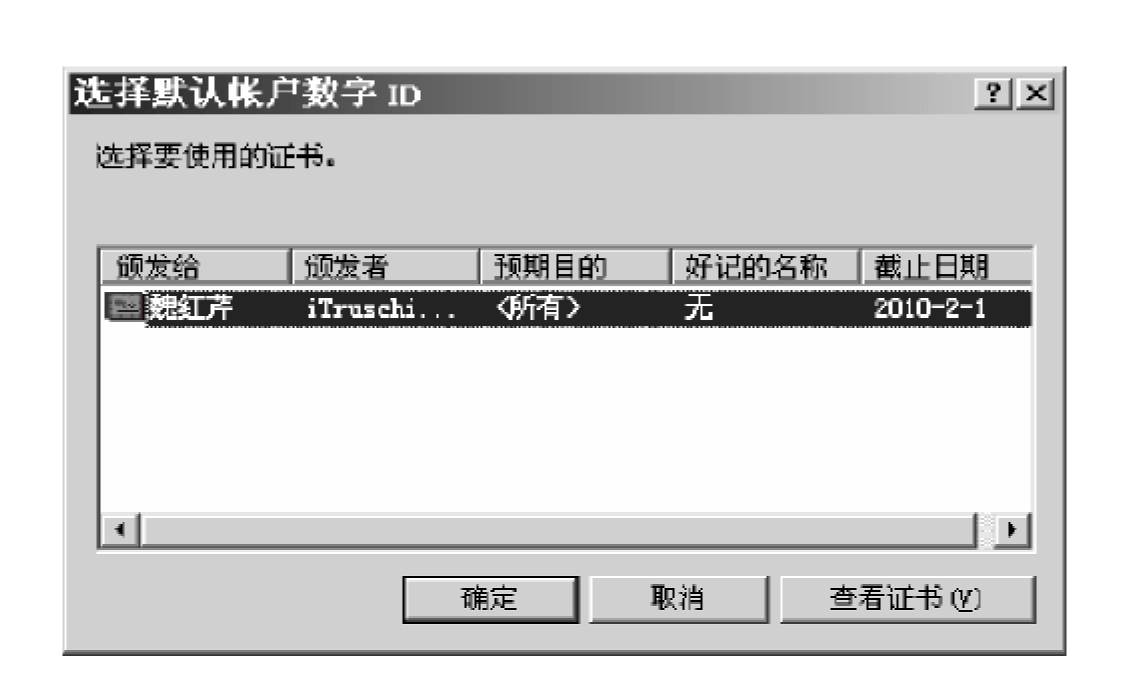


图 4.63 设置邮件签名证书

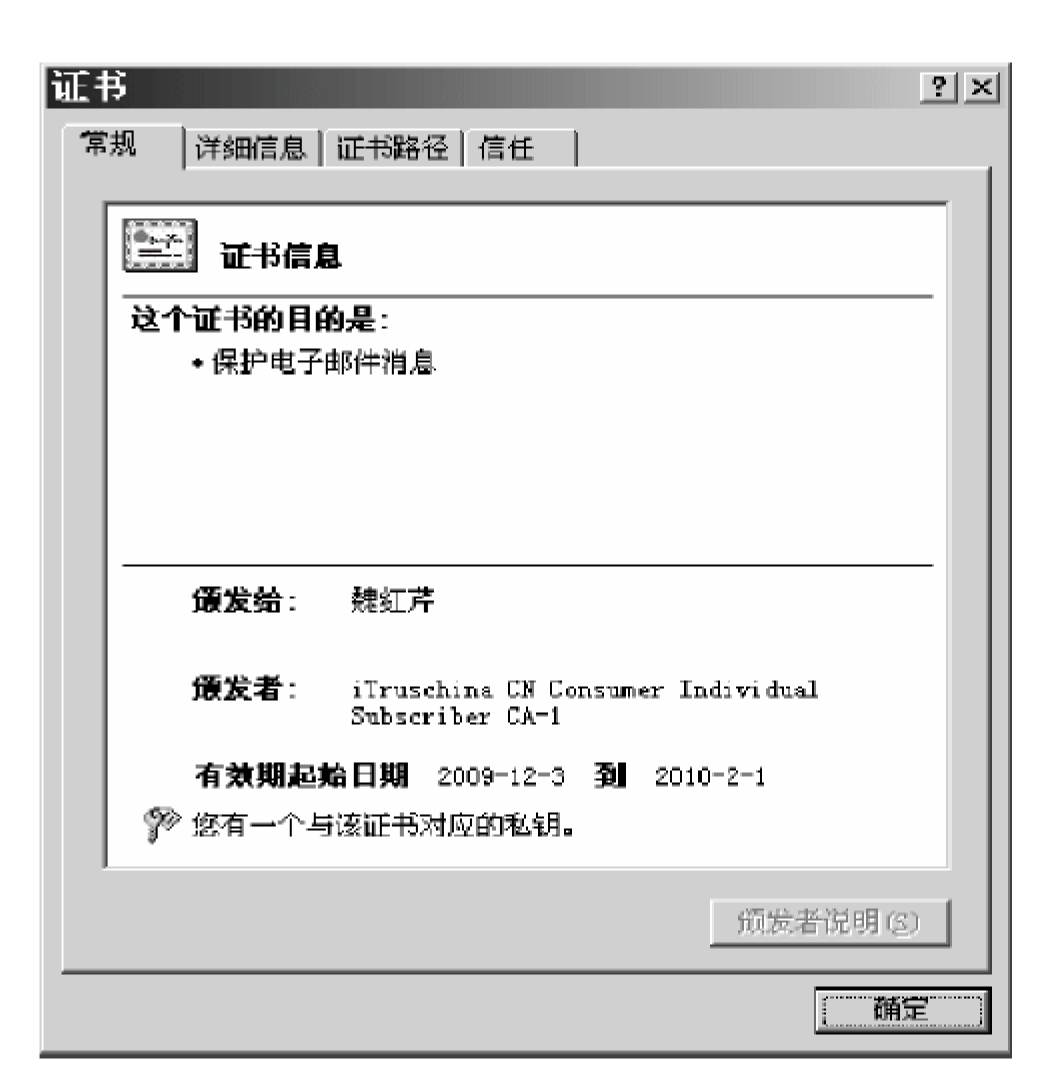


图 4.64 查看签名证书信息

（5）按照同样的方法，也可以在“加密首选项”选项区域中把自己的证书选中，如图 4.65 所示。

（6）发送安全的加密邮件之前，需要先获得接收方的数字标识。可以首先让接收方发送一份签名邮件来获取对方的数字标识，或者直接到电子商务安全认证中心的网站上查询并下载对方的数字标识。然后在该联系人的属性对话框“数字标识”选项卡中，导入其公钥（数字证书），即完成公钥与该联系人的绑定，如图 4.66 和图 4.67 所示。

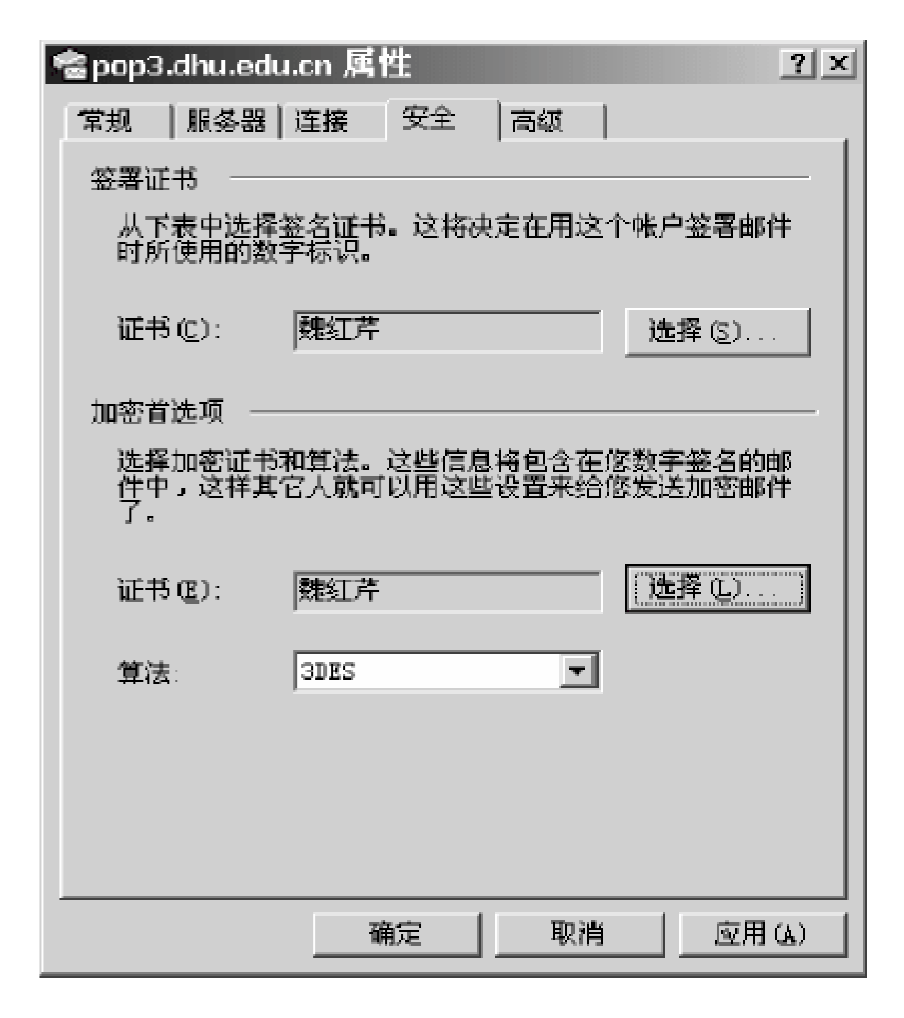


图 4.65 设置邮件加密证书



图 4.66 设置邮件联系人属性



图 4.67 设置邮件联系人数字标识

(7) 在 Outlook Express 6.0 中,单击"创建邮件"按钮,进入"新邮件"窗口,开始撰写邮件。同时选中工具栏中的"签名"或"加密"图标,如图 4.68 所示。

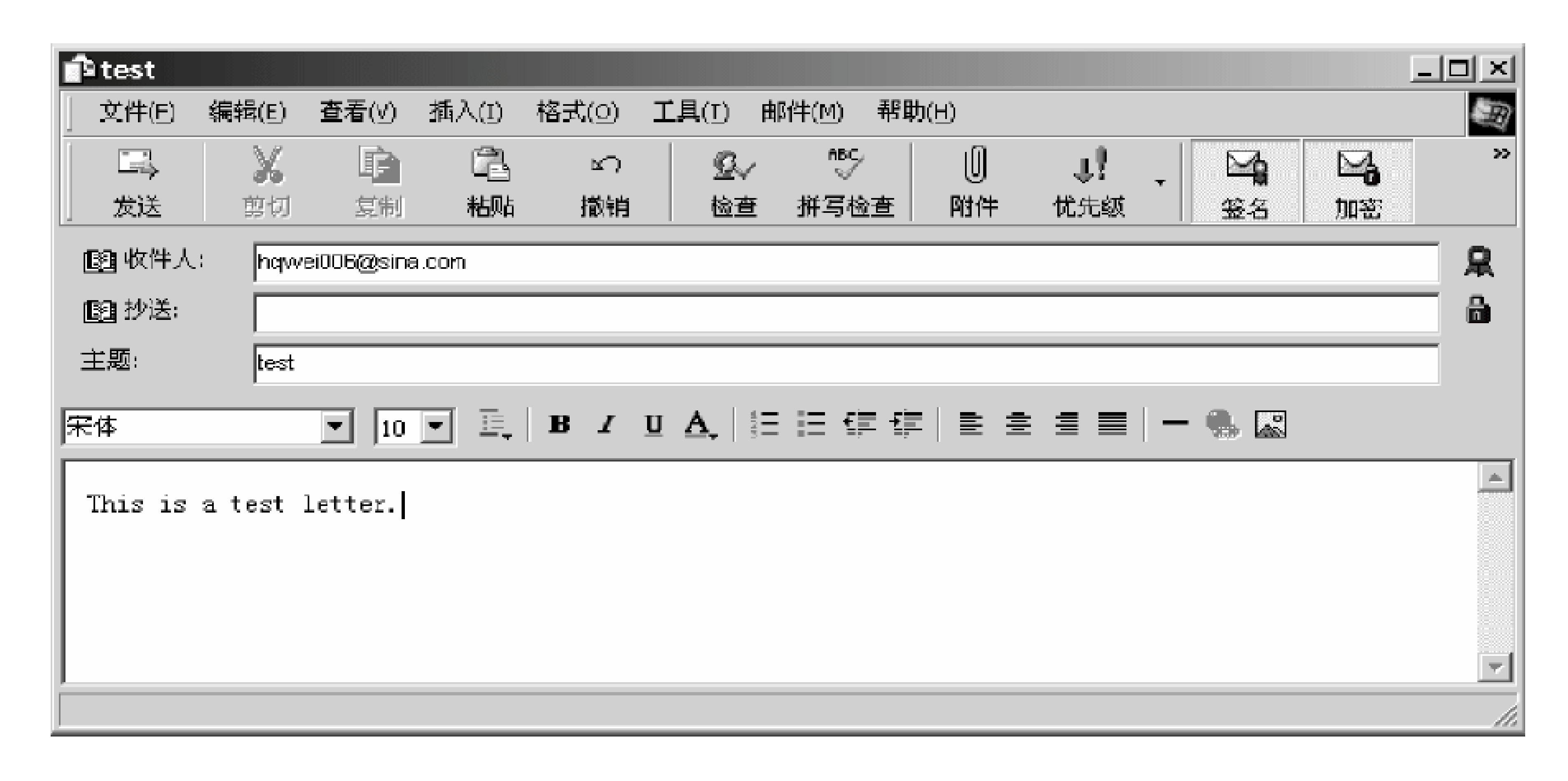


图 4.68 创建加密与签名邮件

(8) 然后单击"发送"按钮,签名邮件的发送即告成功。

(9) 当收件人收到并打开有数字签名和加密的邮件时,对方将看到"数字签名和加密邮件"的提示信息,如图 4.69 所示。只有在单击"继续"按钮后,才可以阅读该邮件内容,如图 4.70 所示。若该邮件在传输过程中被其他人篡改或发信人的数字证书有问题,系统将给出"安全警告"提示。

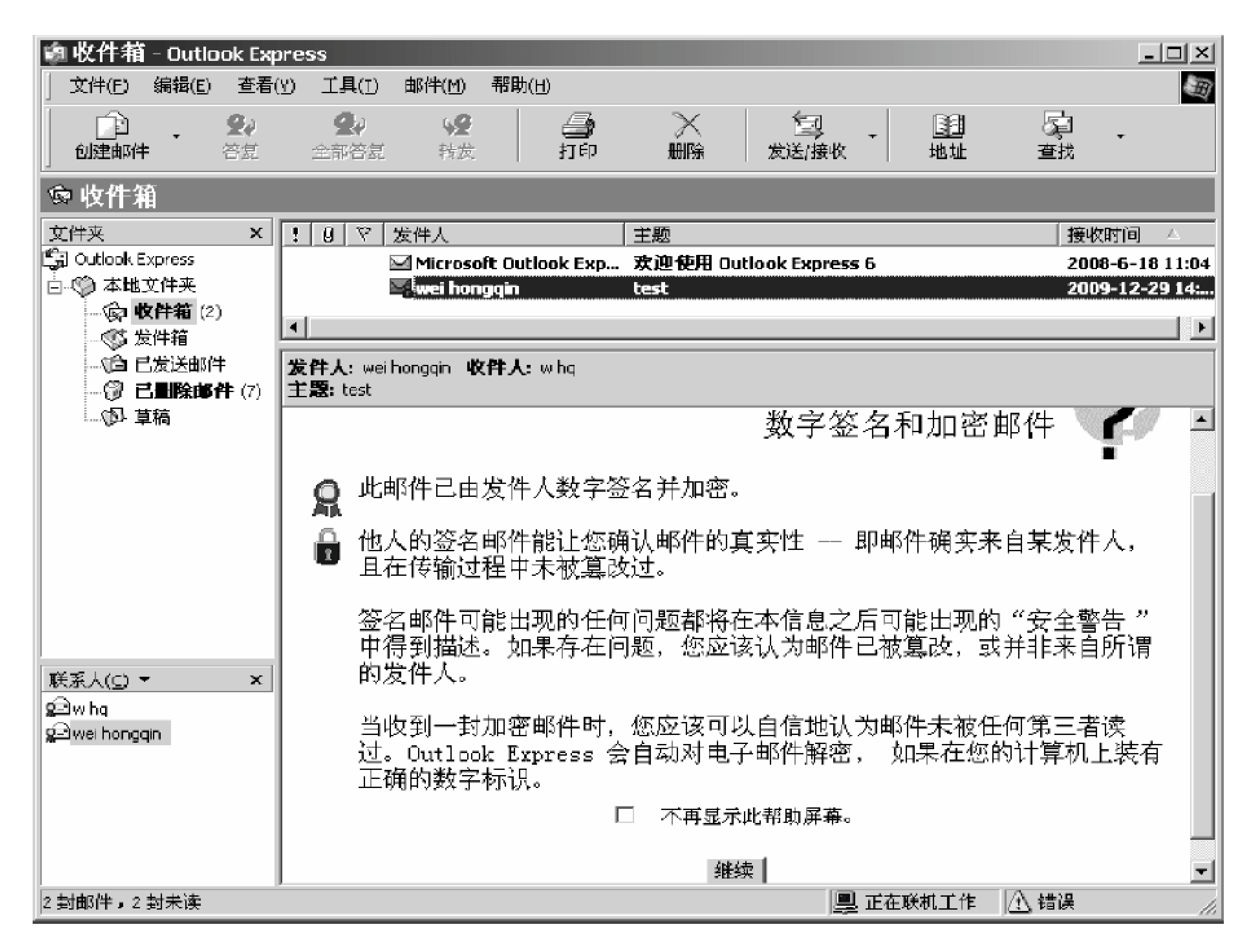


图 4.69 收取数字签名和加密邮件

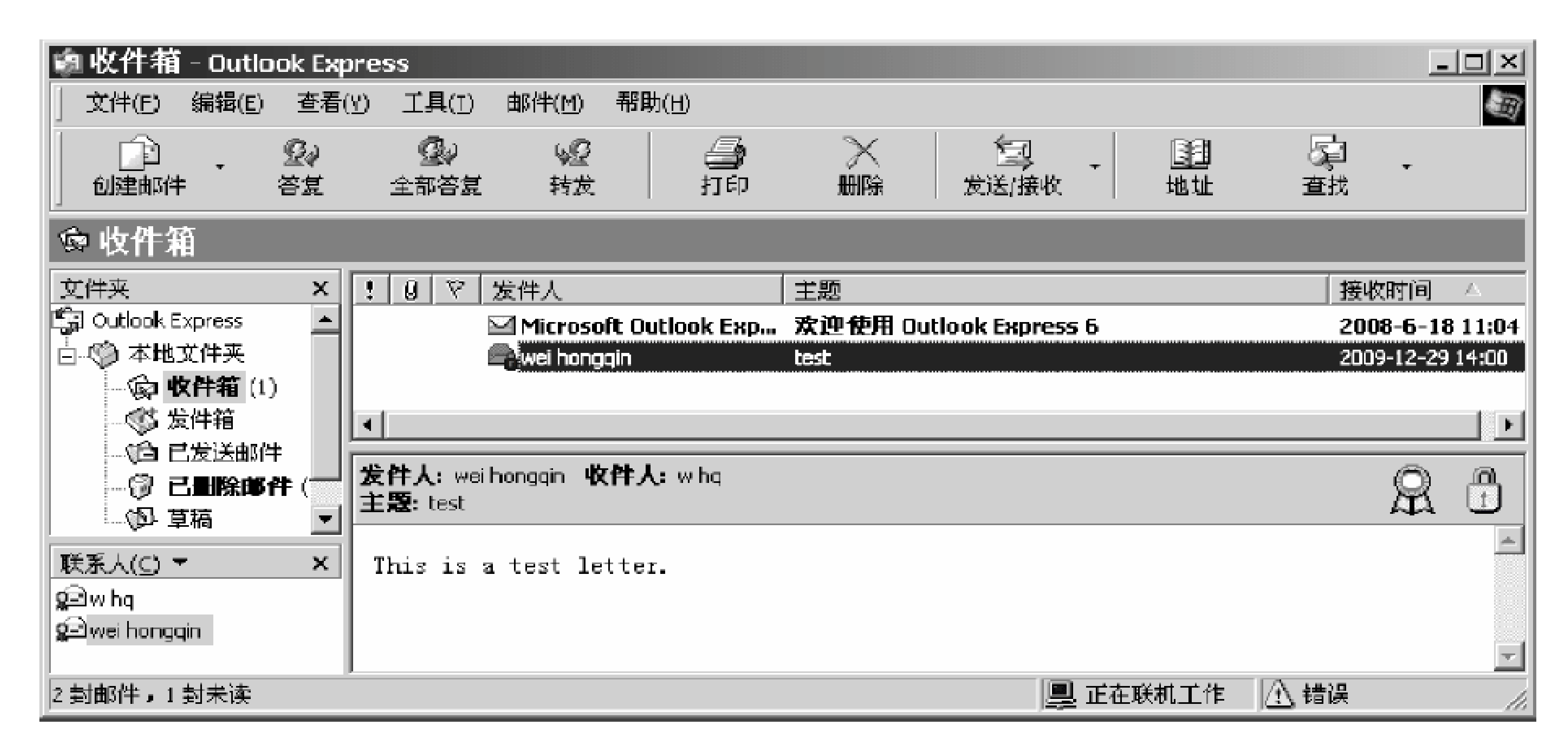


图 4.70 查看加密与签名邮件

（10）在收到具有数字签名的邮件后，可以看到，在邮件窗口的右边中间有一个“数字签名”图标，单击它可以看到相关的数字证书信息，如图 4.71 和图 4.72 所示。

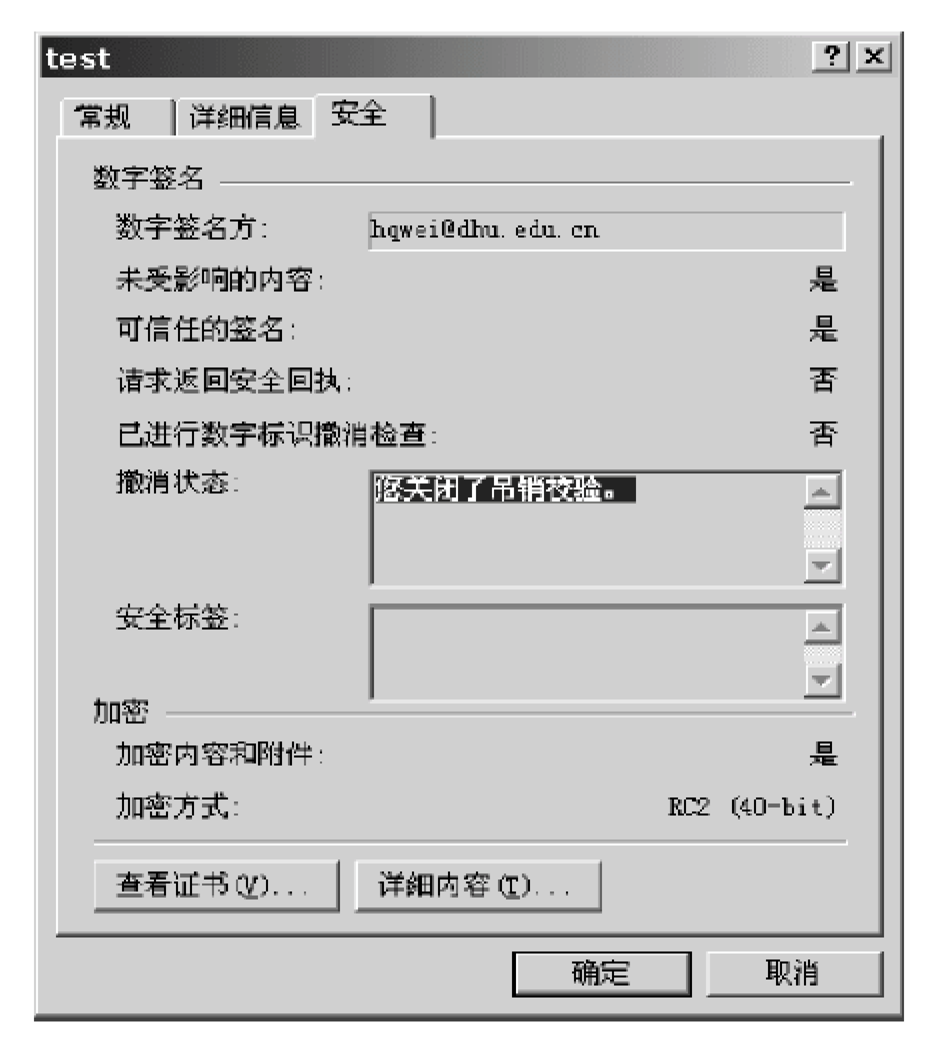


图 4.71　查看数字签名信息



图 4.72　查看证书信息

6. 实验报告与要求

在 Outlook 中用另一用户或实验教师的公钥给对方发送一封带签名和加密的邮件，同时将自己的公钥放在附件中。

7. 实验分析与讨论

数字证书的生命周期包含申请、使用、查询、吊销等过程，本实验仅涉及申请、安装和使用，用户可以结合 PKI 的基本构成和主要职能自行尝试 CA 中心所提供的其他数字证书服务功能。另外，用户可以考虑除个人电子邮件证书外，还有哪些类型的数字证书，应该如何安装和使用。

8. 注意事项

（1）选择邮箱的签名和加密证书时，如果单击"选择"按钮，没有相关的数字证书弹出，请确认您的证书已经正确安装且没有过期。同时还要确认您在 Outlook Express 中所设置的邮箱与您在申请数字证书时所提供的邮箱是一致的。查看在申请数字证书时所使用的邮箱方法是，在 Internet Explorer 中，选择"工具"|"Internet 选项"|"内容"|"证书"命令，选中数字证书后，依次选择"查看"|"详细信息"|"主题"即可。

（2）为联系人添加数字证书时，收信地址需要与联系人证书中的邮件地址相同。

（3）发送加密邮件的方法与发送签名邮件的方法类似，也可以对即将发送的同一封邮件既签名又加密，两种方式可以同时使用。

（4）在 Outlook 中发送邮件时，应注意电子邮件服务器设置的正确性，以保证邮件可以顺利发出。

（5）不同 CA 中心的证书申请流程和方法会有一些差异，而基本的流程是相似的，通

常需要用户填写个人基本信息，然后需要安装根证书链，最后获取个人数字证书并进行安装。

4.2.4 PGP 软件使用

1. 实验目的

了解 PGP 软件的基本功能，掌握软件使用方法。

2. 实验原理

本实验选用 PGP 软件的免费版本 PGP6.5.3。

3. 实验环境

实验者两两结合形成小组，合作完成密钥的使用。

4. 实验内容

(1) PGP 软件安装；
(2) PGP 密钥对管理；
(3) 使用 PGP 密钥对加解密；
(4) 使用 PGP 对信息进行签名和认证；
(5) PGP 加密、签名电子邮件；
(6) 利用 PGP 进行磁盘和文件清理。

5. 实验步骤

1) PGP 软件安装

(1) 双击 pgp 6.5.3-Setup.exe，按照默认提示进行安装，如图 4.73～图 4.75 所示。

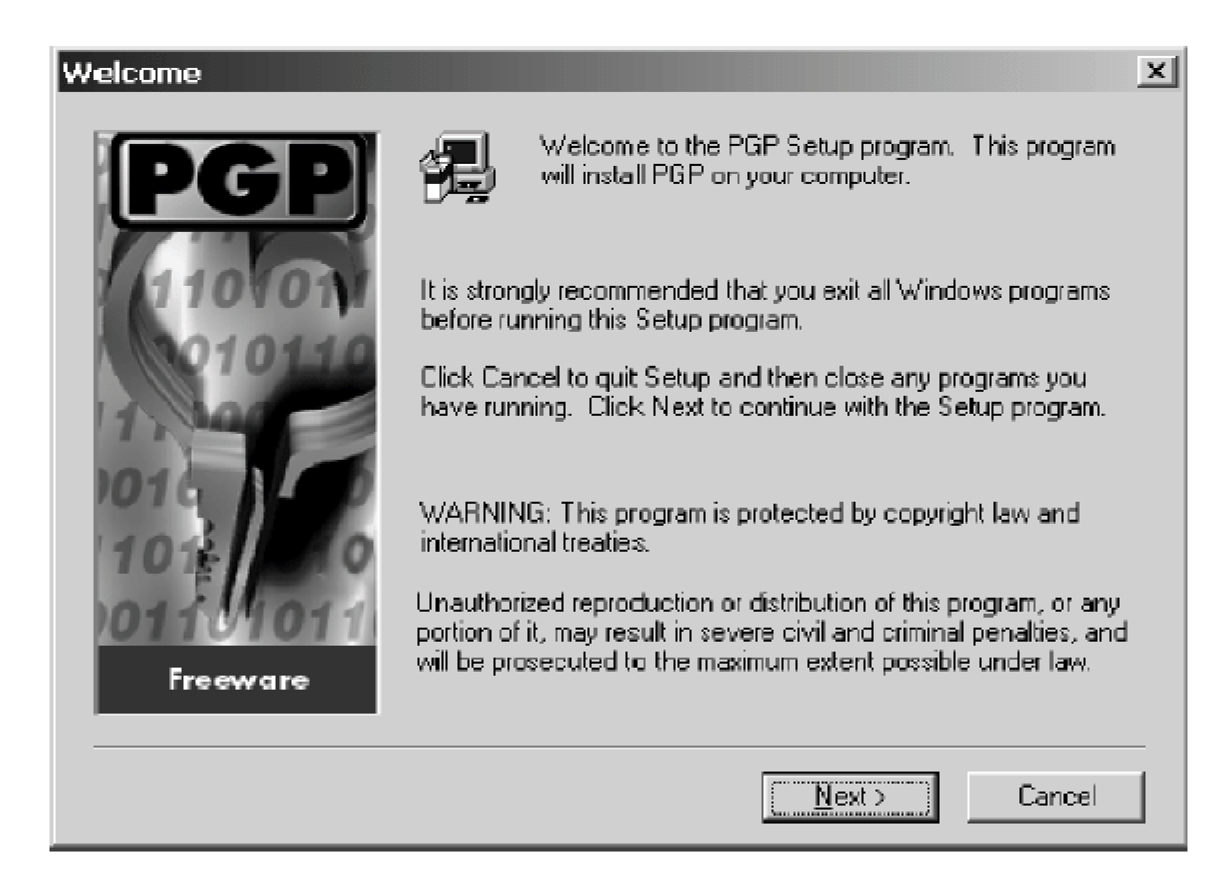


图 4.73 安装 PGP 软件

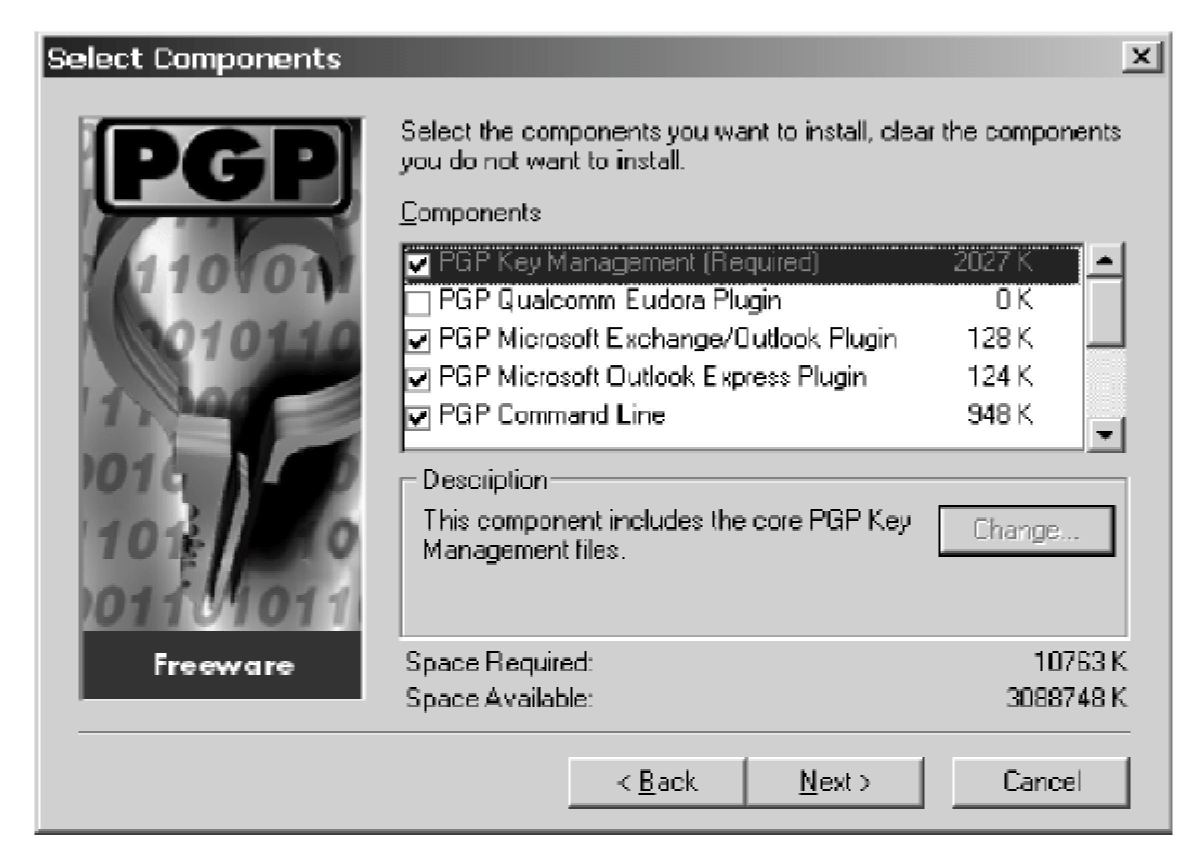


图 4.74　设置关联程序



图 4.75　完成 PGP 安装

（2）第一次安装完成后，依照提示生成自己的密钥对，如图 4.76～图 4.81 所示。



图 4.76　密钥生成向导



图 4.77 生成新的密钥

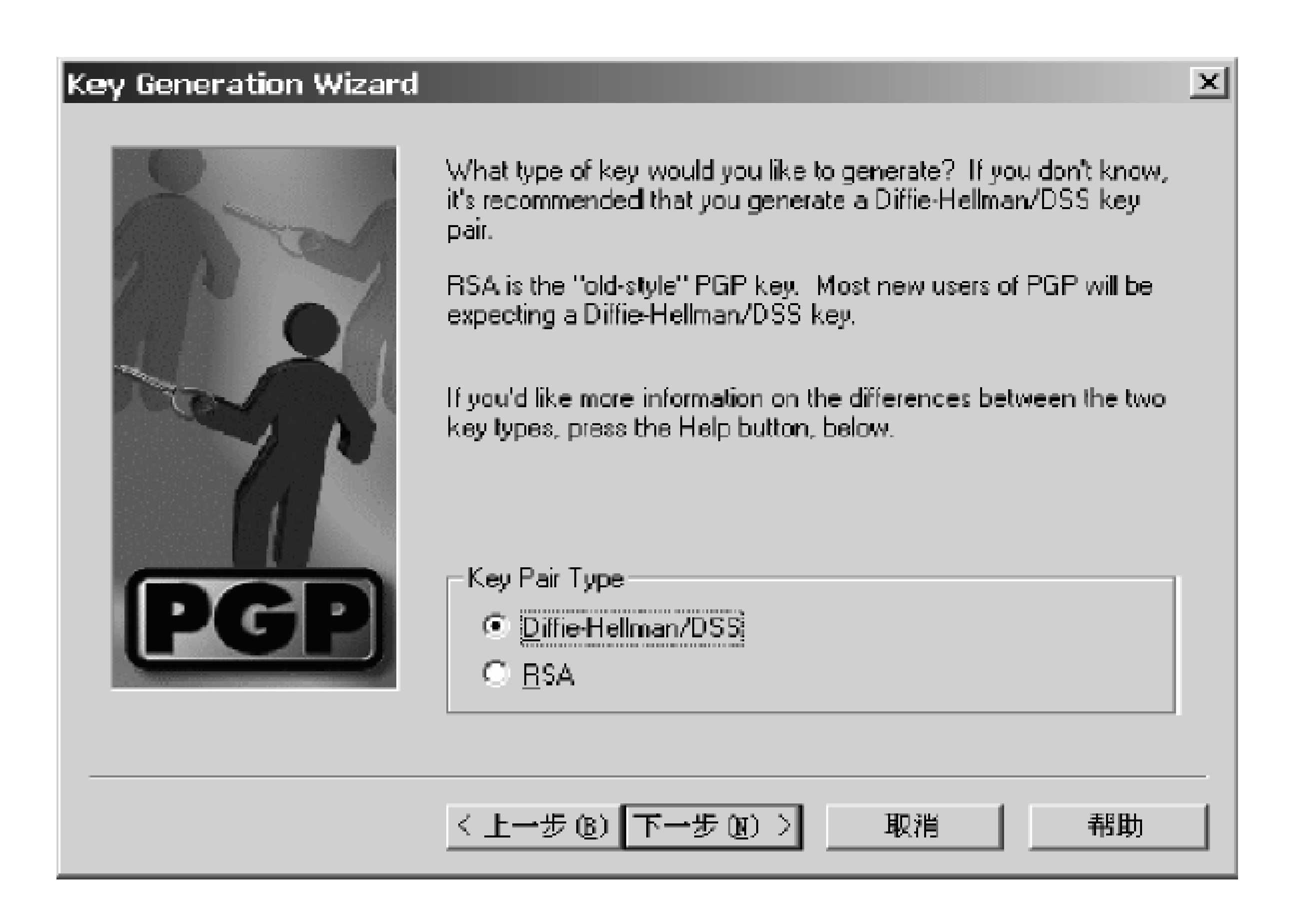


图 4.78 设置密钥生成算法



图 4.79 设置密钥有效期

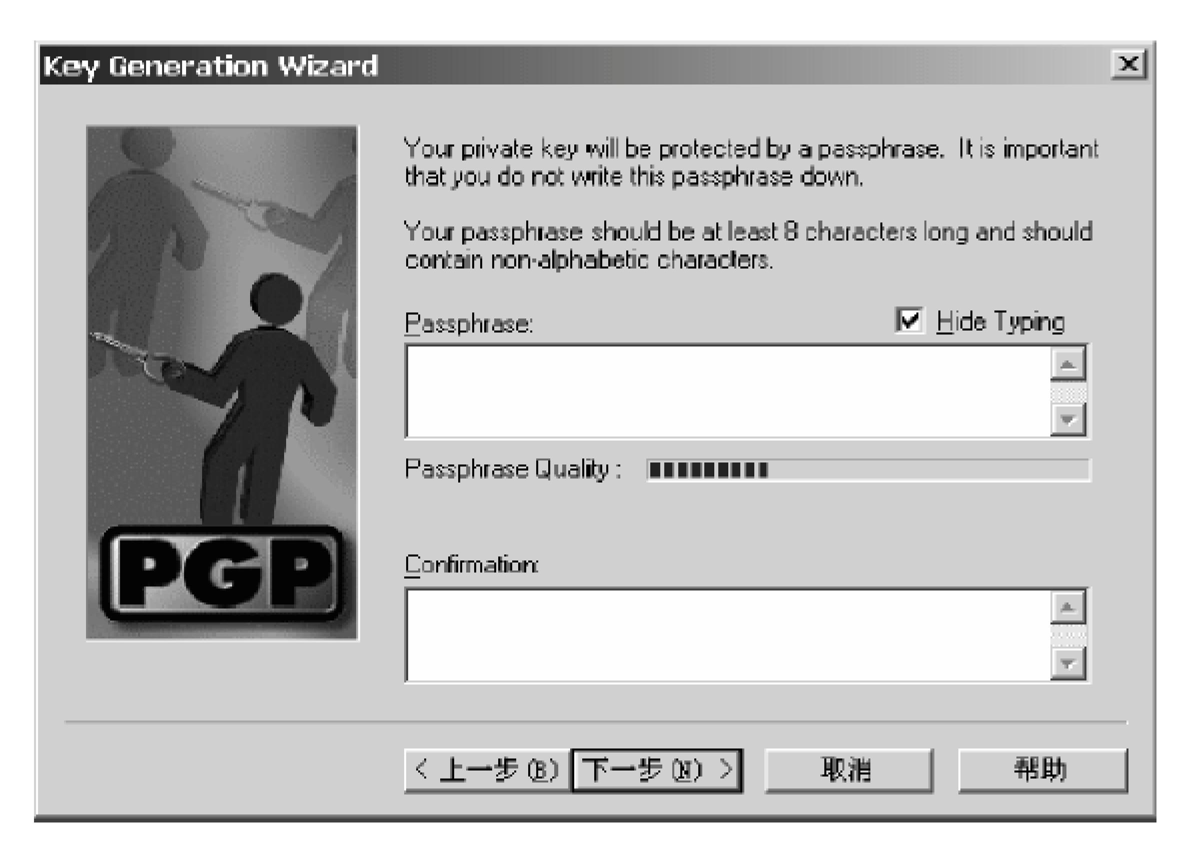


图 4.80　设置密钥口令



图 4.81　完成密钥生成

2）PGP 密钥对管理

（1）在"程序"|"启动"选项中选中 pgptray 命令加载 PGP 程序。

（2）单击桌面右下角锁形图标，选择 PGPkeys 选项，进入密钥管理界面，查看密钥列表，如图 4.82 所示。

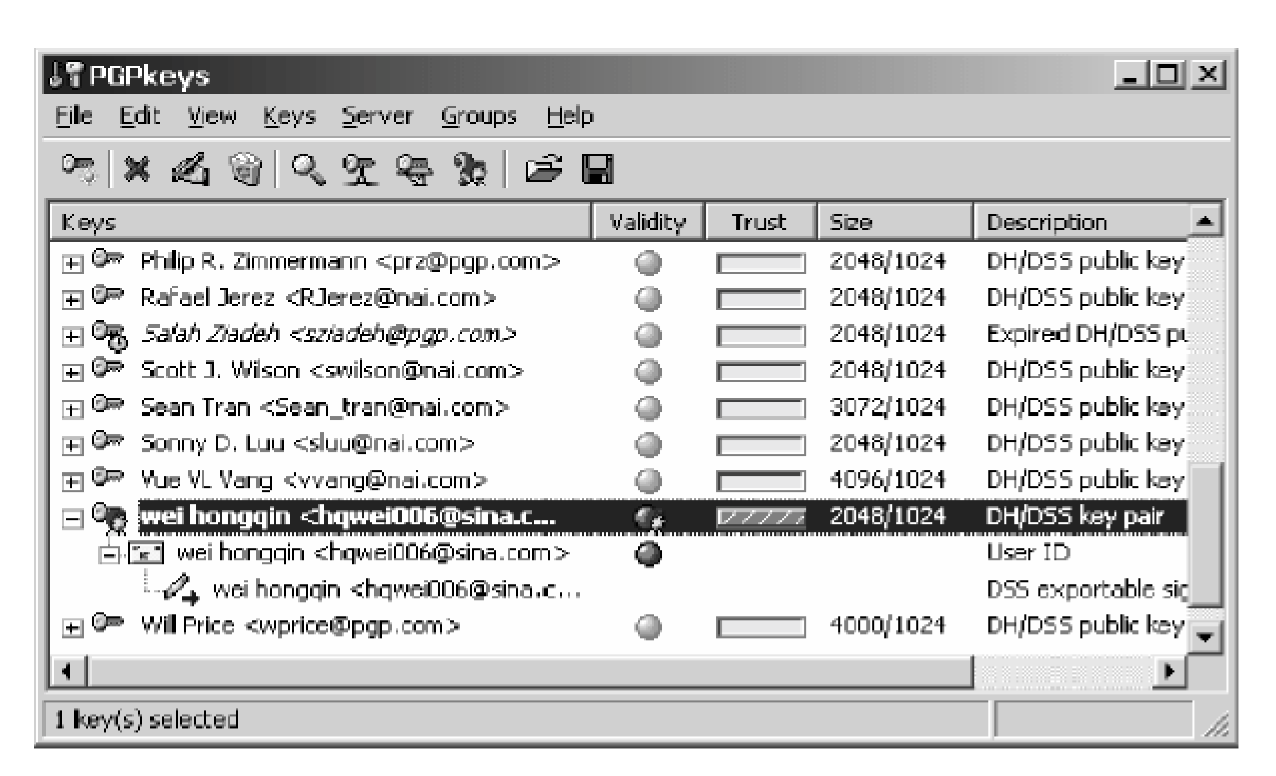


图 4.82　查看密钥列表

（3）选择 Keys|New Key 或相应图标，创建多个新密钥对，如图 4.83 所示。

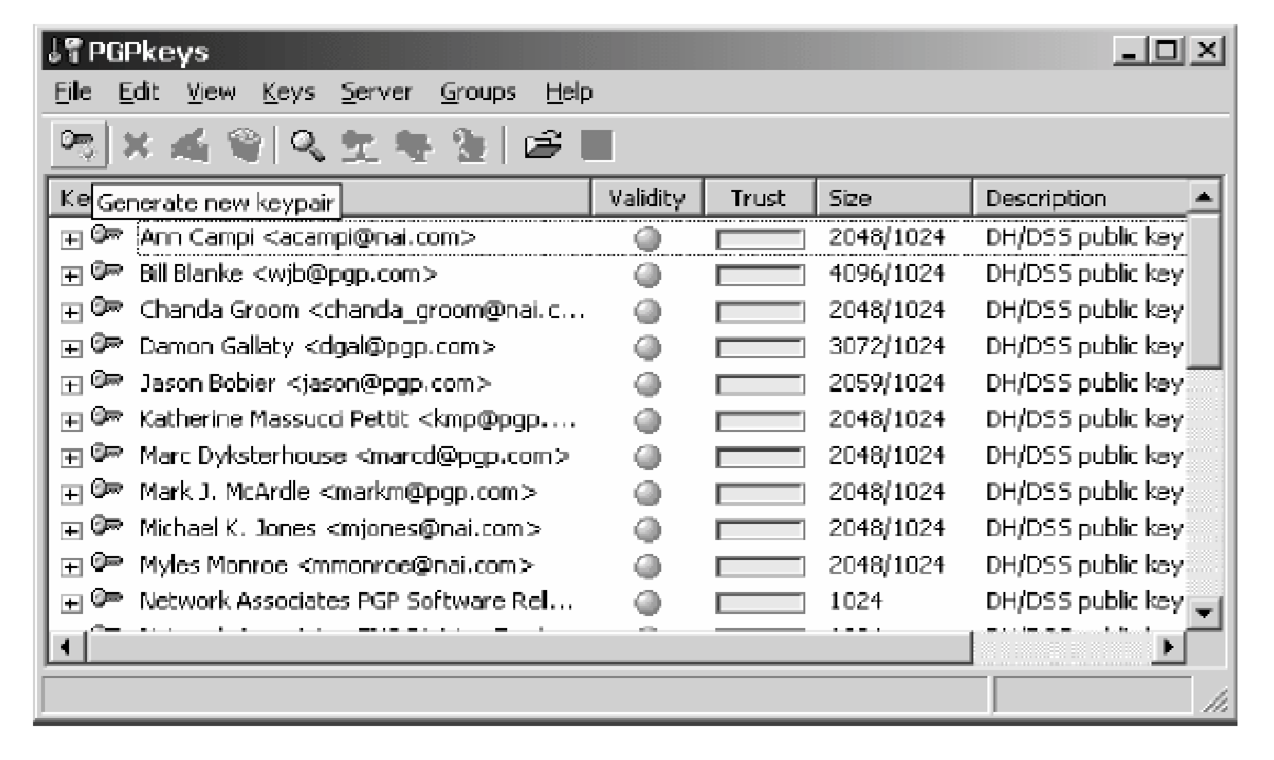


图 4.83　创建密钥对

（4）选中密钥，右击，选择 Revoke 或在菜单中选择 Keys|Revoke，废除该密钥对，如图 4.84 所示。

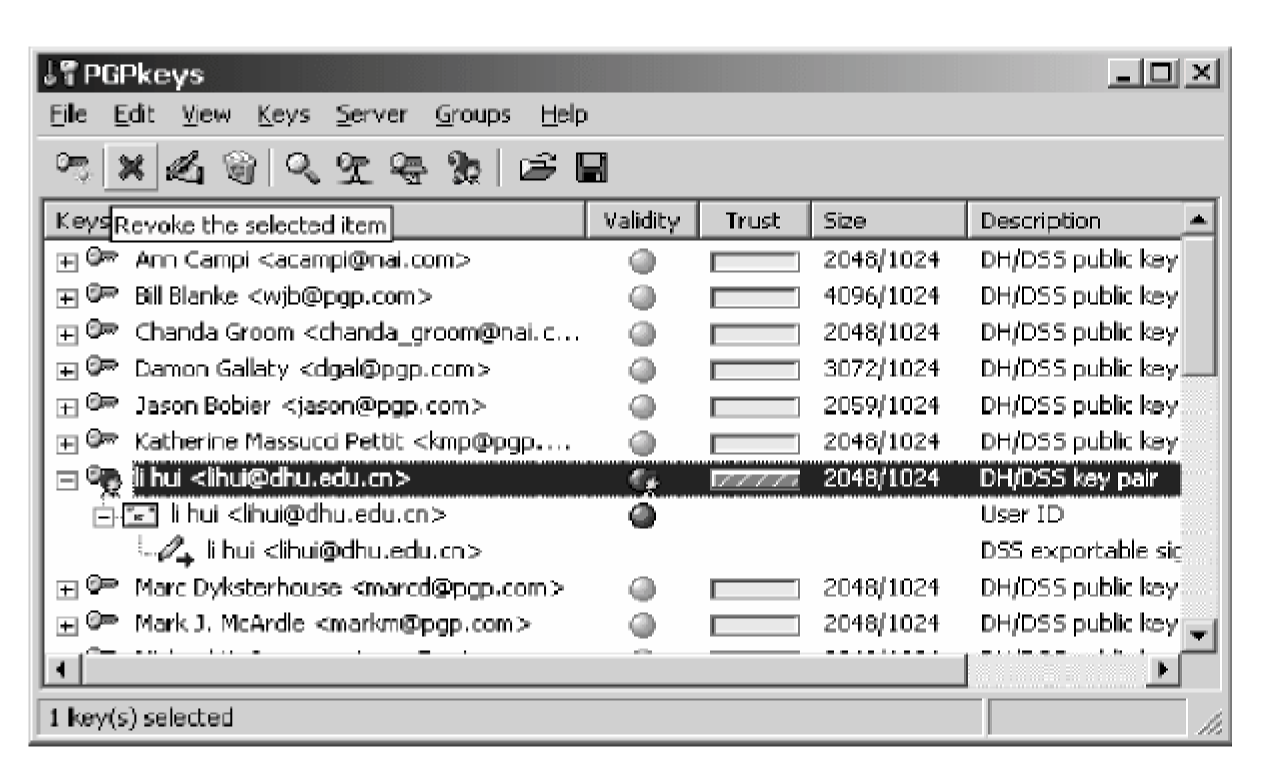


图 4.84　废除密钥

（5）选中密钥，右击，选择 Share Split 或在菜单中选择 Keys|Share Split，按照提示选择分量个数和存储位置，将该密钥对拆分成几个分量，分别保存，如图 4.85 和图 4.86 所示。

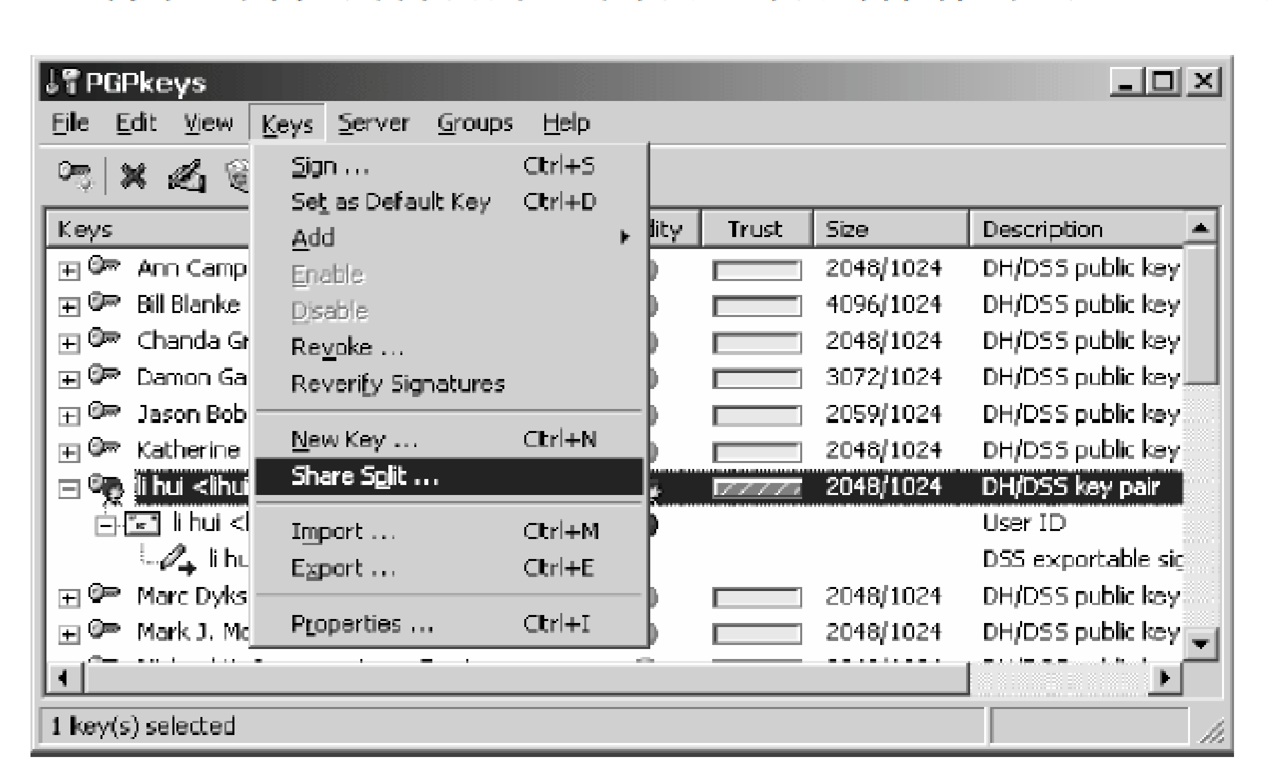


图 4.85　拆分密钥(1)



图 4.86　拆分密钥(2)

(6) 选中密钥,右击,选择 Export 或在菜单中选择 Keys|Export,导出自己的一把 PGP 公钥,与小组内另一实验用户交换,并用 Import 命令把对方公钥导入自己的 PGPkeys 中,如图 4.87～图 4.89 所示。

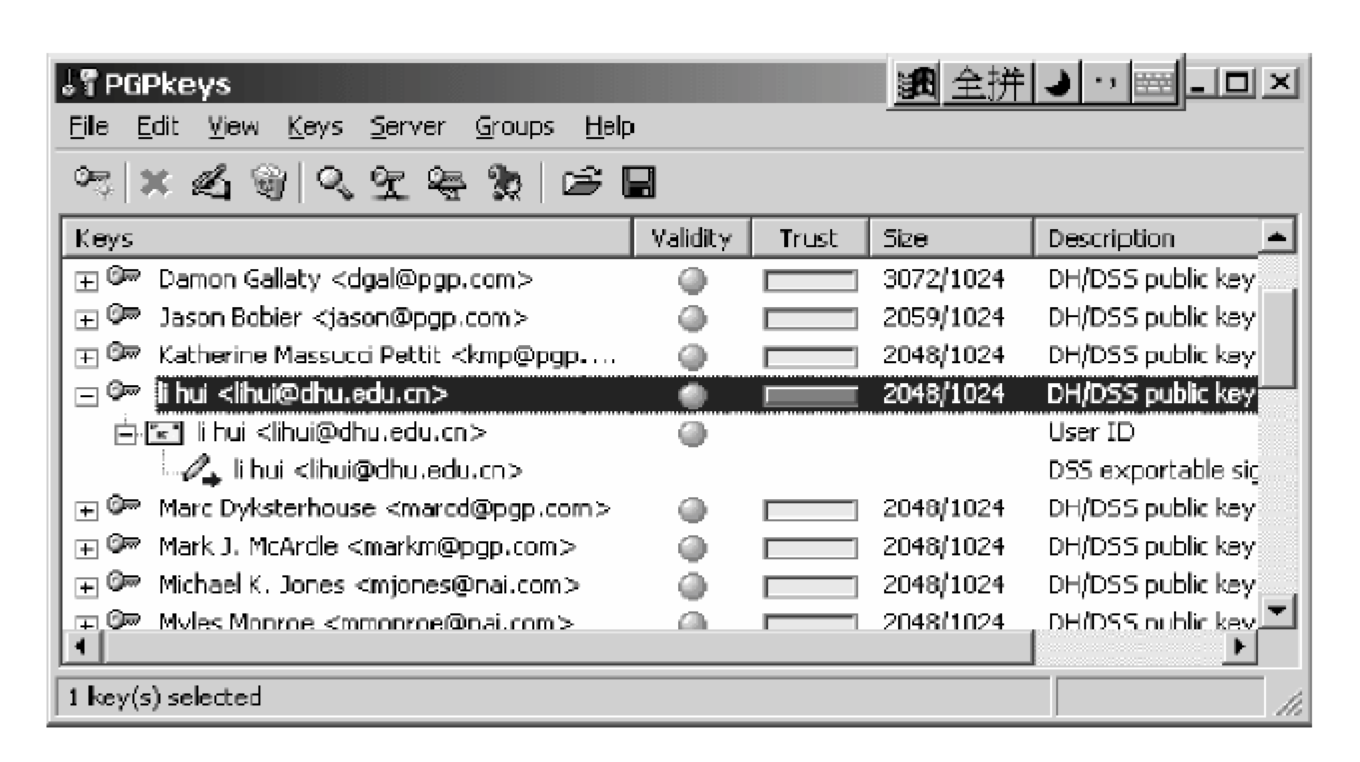


图 4.87　选择密钥进行导出

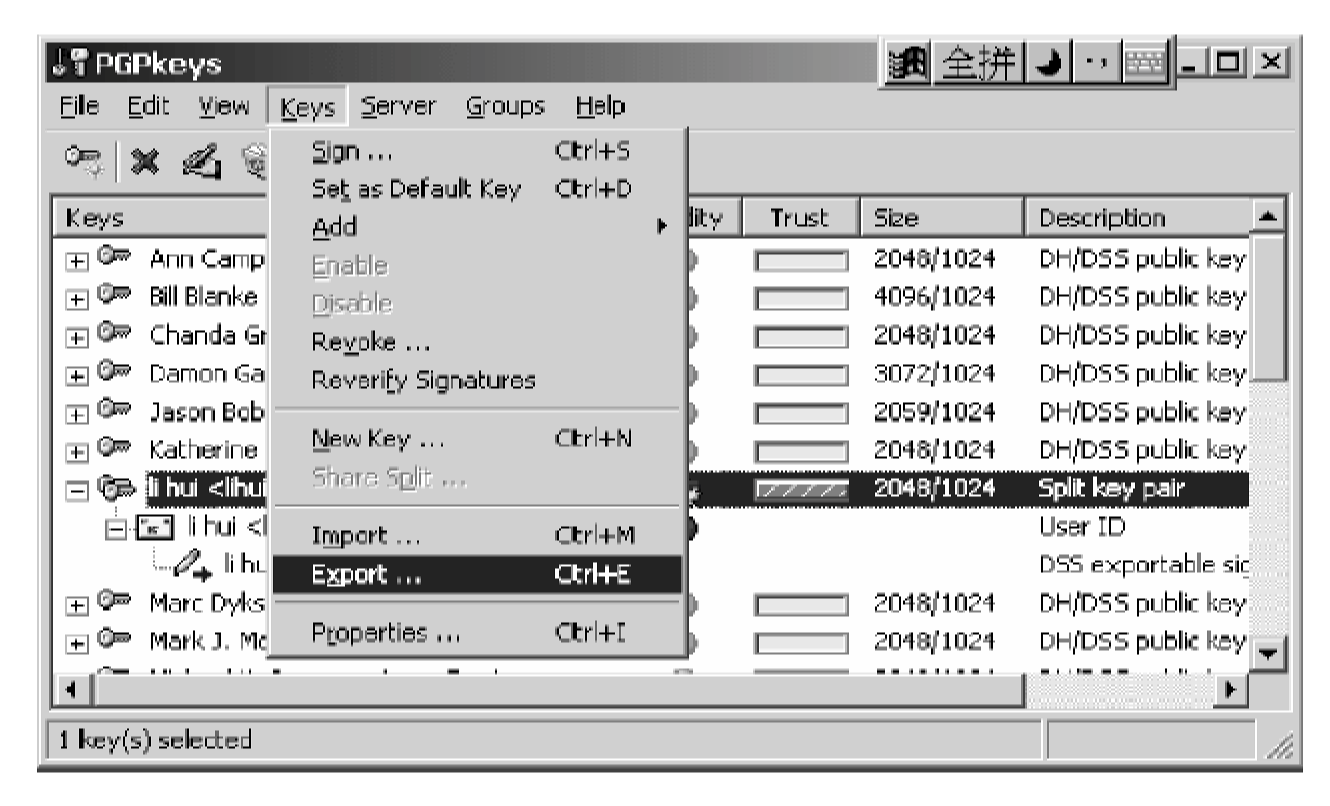


图 4.88　导出密钥

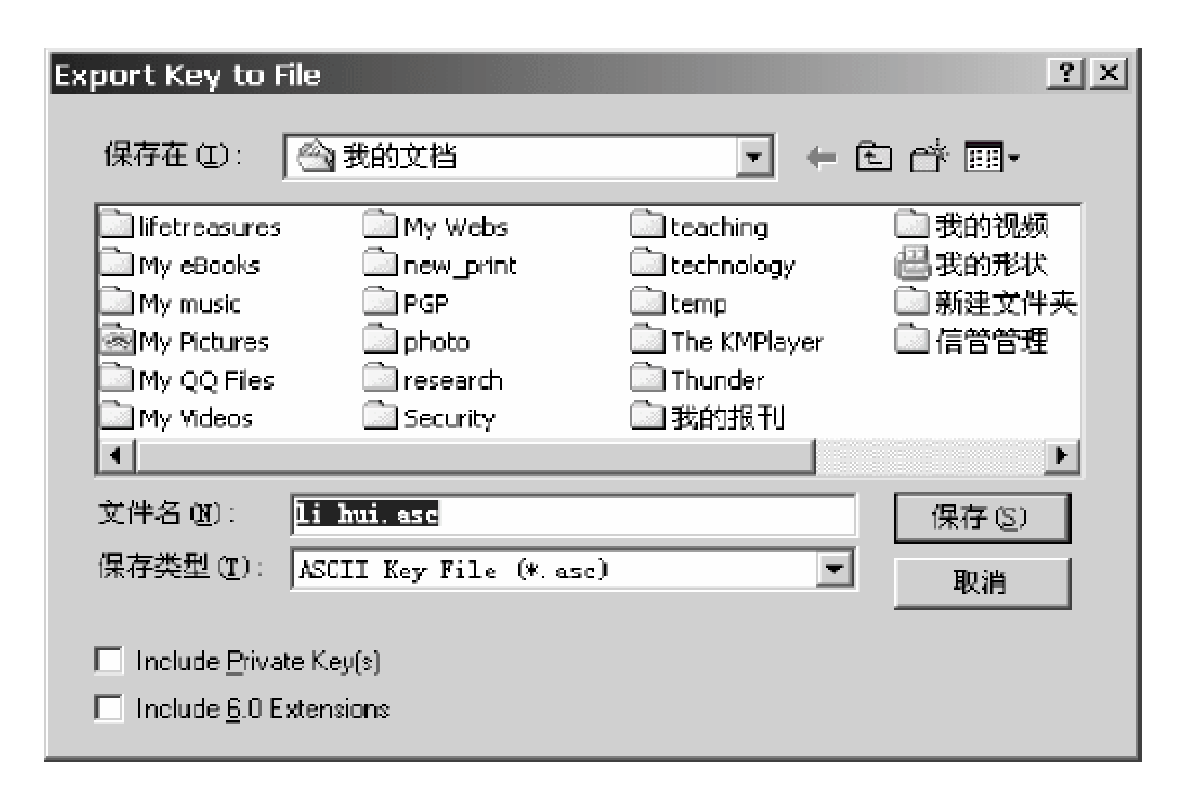


图 4.89 保存密钥到文件

3）使用 PGP 密钥对加解密

（1）在桌面右下角图标 PGPtray|Current Windows 中选择相应命令，使用 PGP 对某打开的文本中部分信息进行加密（加密时选用实验对方的公钥），如图 4.90 和图 4.91 所示。

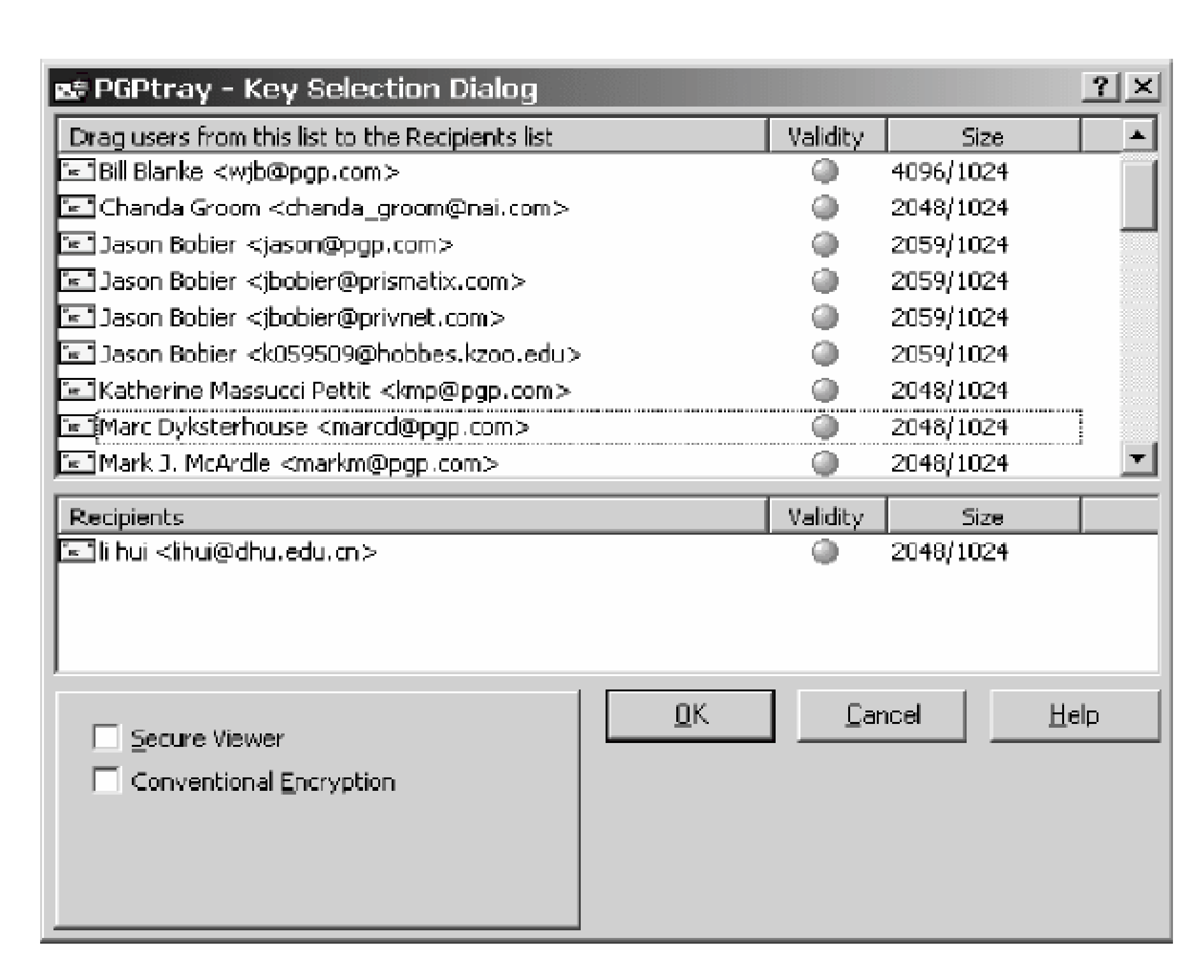


图 4.90 选择加密密钥

（2）实验对方对收到的加密信息，用同样方法对其解密读取（用自己的私钥）。

（3）选中某文件或文件夹后，右键选择 PGP 菜单中的命令 Encrypt，对该文件夹或文件进行加密，加密时选用实验配合方的公钥。

（4）实验对方用同样方法选择 Decrypt 命令对加密内容解密读取（用自己的配套私钥）。

4）使用 PGP 对信息进行签名和认证

（1）对信息、文件或文件夹右键选择 PGP 菜单中的 Encrypt & Sign 进行签名后，发给实验配合方进行验证，操作方法同上。

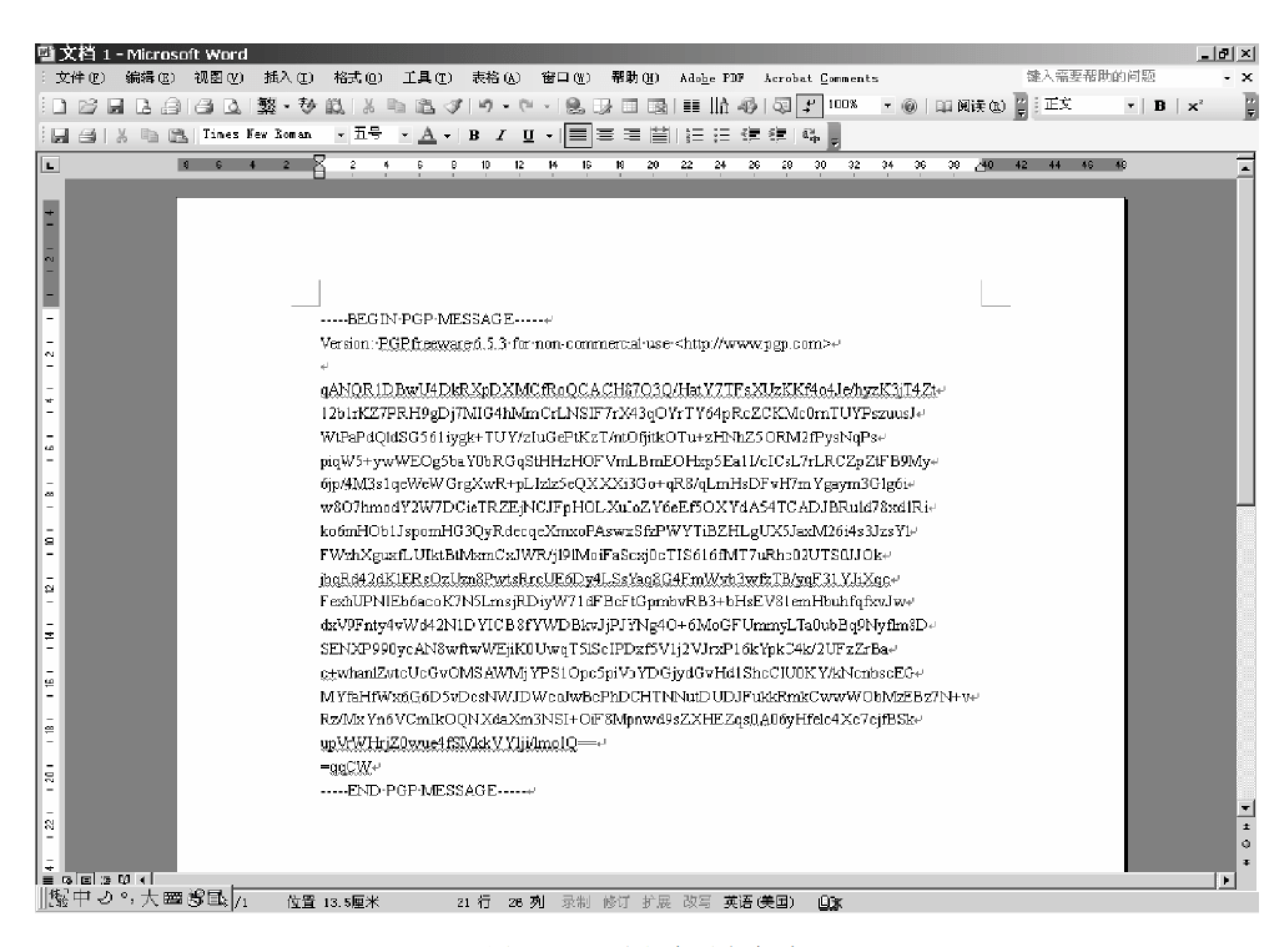


图 4.91　对文本进行加密

（2）选中自己信任的某同学的公钥，单击 Sign 命令进行签名并 Import 导出返还给对方，对方可以得到被第三方信任签名的密钥，如图 4.92 所示。

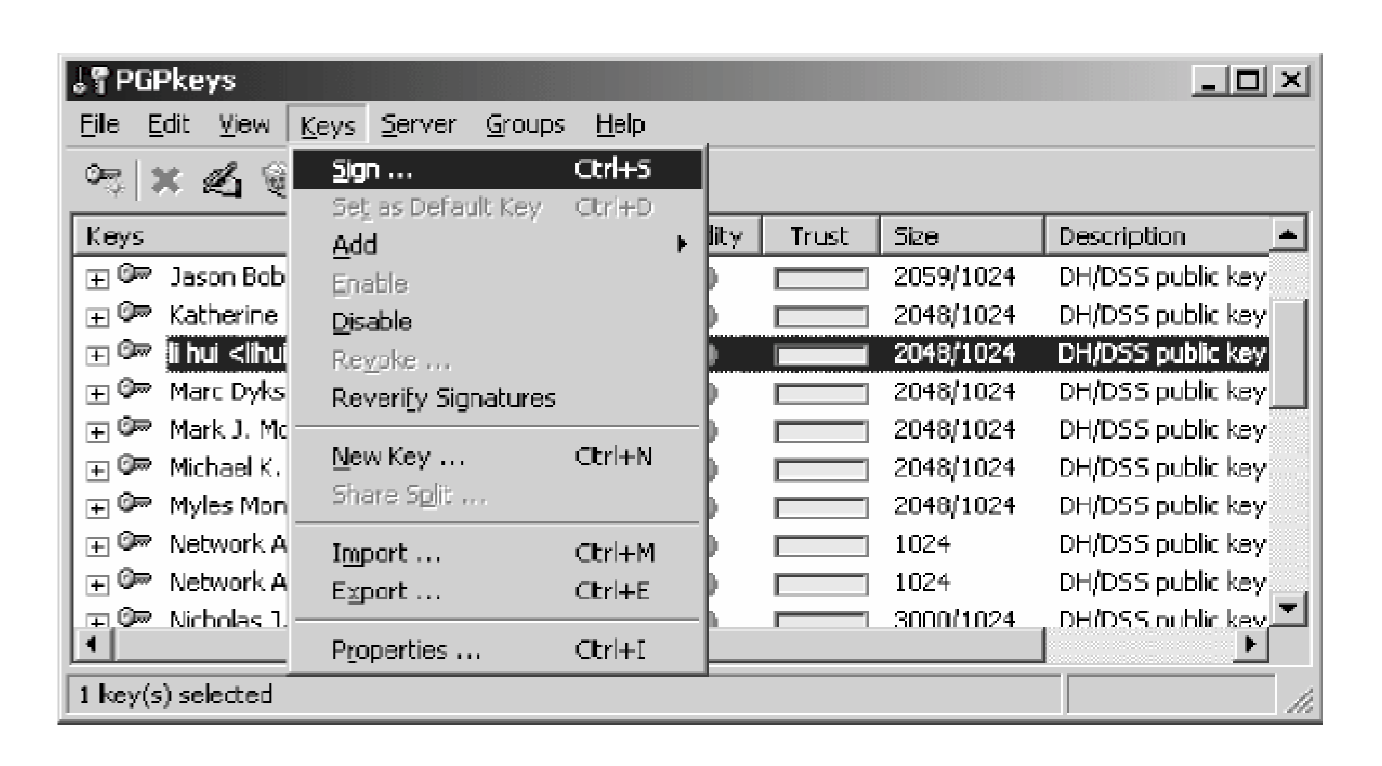


图 4.92　对密钥进行签名

5）实验小组双方 PGP 加密、签名电子邮件

（1）打开邮件服务软件，撰写新邮件，选中邮件主题部分，单击 PGP 工具中的 Encrypt 和 Sign 命令，对邮件进行加密和签名，然后发送给对方。

（2）对方解密读取收到的邮件，并对发信人身份进行认证，如图 4.93 所示。



图 4.93 对邮件进行加密和签名

6）利用 PGP 进行磁盘和文件清理

（1）选择桌面右下角 PGP 图标中 PGPtools 命令，打开工具面板，如图 4.94 所示。



图 4.94 PGP 工具面板

（2）单击 Wipe 图标，选择需要清除的文件，如图 4.95 所示。



图 4.95 清除文件

（3）单击 Free Space Wipe 图标选择需要清除信息的磁盘，如图 4.96～图 4.98 所示。

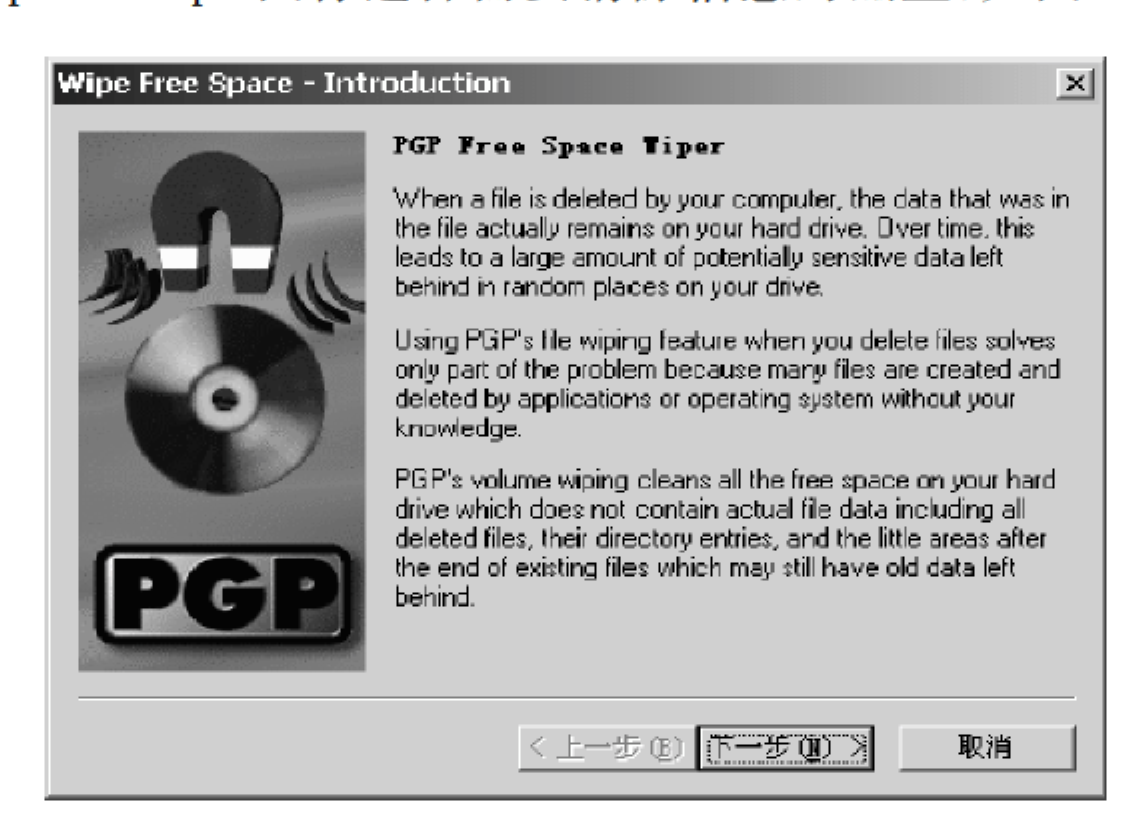


图 4.96　清除磁盘信息

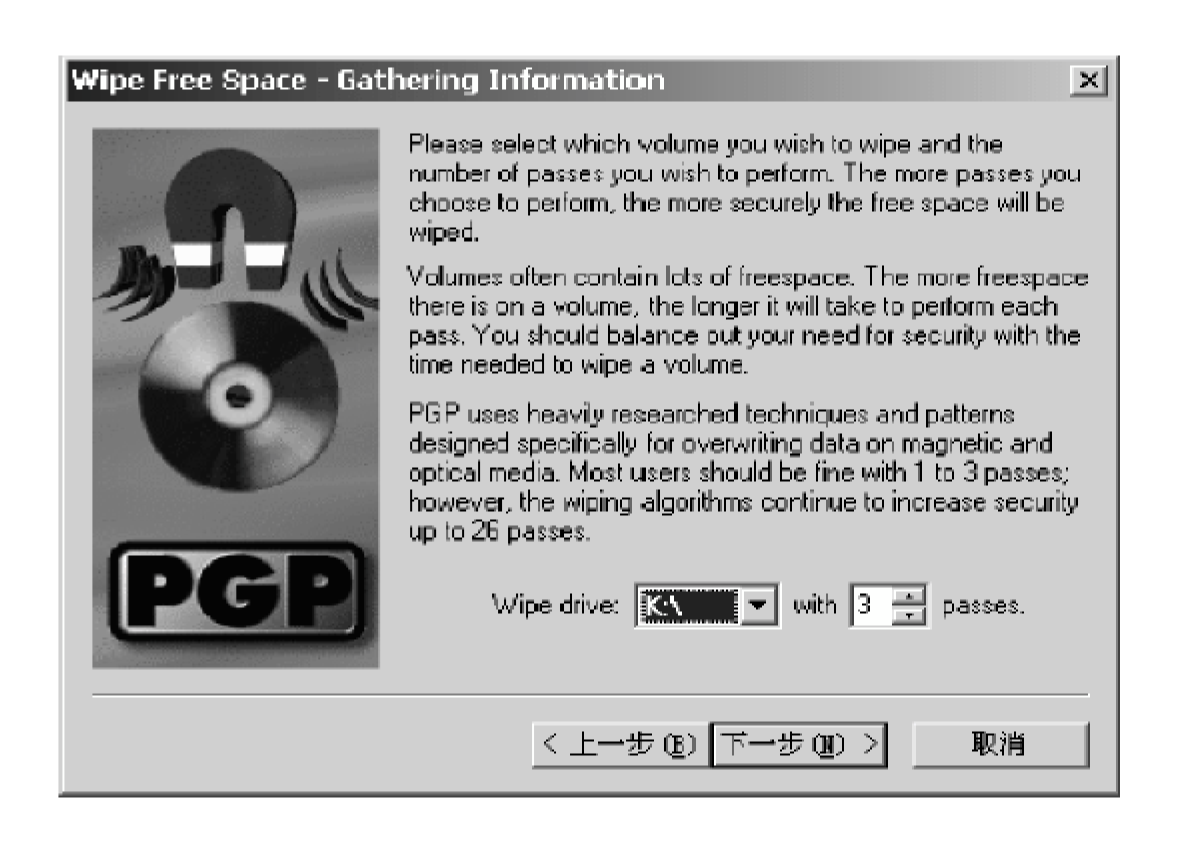


图 4.97　设置清除磁盘参数



图 4.98　执行磁盘信息清除

6. 实验报告与要求

将另一实验用户或实验教师公钥导入自己的 PGP 系统，在 Outlook 中用该公钥给对方发送一封带签名和加密的邮件，同时将自己的公钥放在附件中。

7. 实验分析与讨论

请用户考虑利用 PGP 进行电子邮件加密时，保护的是什么内容，发信人和收信人的地址信息是否可以被加密，为了实现更为全面的电子邮件安全，可以采取什么方法。

8. 注意事项

(1) 为使 PGP 工具可以内嵌入 Outlook 程序，安装时需要选中相应的支持组件。

(2) PGP 成功安装并重启后，桌面右下角会出现一个锁形的 PGP 图标；如果没有重启，则可以在“程序”|“启动”项中加载 PGPtray。

(3) 进行密钥导出时，不选中 Include Private Key 就可以仅导出公钥；对于导出的密钥，要在另一系统中使用时，可以用 Import 命令导入。

(4) 拆分密钥可以在不同地点进行密钥分量的保管，密钥被拆分后，以后每次使用前都需要首先将各分量组合起来，因此拆分密钥会增加使用的复杂性，但会提高密钥的安全性。

(5) 实验时，邮件发送可以在 Outlook 中或其他邮件网站上进行，对邮件正文部分签名并加密后发出。如果对方没有自己的公钥，需要作为附件发出。

(6) 加密信息时，发送方需要选择接受方的公钥，签名信息时，则需要选用自己的私钥；解密信息时，接受方需要选用自己的私钥，验证签名信息时，则需要选用发送方的公钥。

(7) PGP 中的 Wipe 功能可以更加彻底地清除磁盘文件信息，防止数据恢复工具获取已删除的有用信息。进行磁盘清除时，选择的清除次数越高，数据清除安全性越好，但需要的操作时间会越长。

4.2.5 数据库安全

1. 实验目的

了解和掌握 SQL Server 2000 的安全配置方法。

2. 实验原理

Microsoft 公司的 SQL Server 2000 是一种广泛使用的数据库，相对信息安全的其他领域，数据库安全经常会被用户甚至系统管理员忽视。数据库系统中存在的安全漏洞和不当的配置通常会造成严重的后果，而且较难被发现。SQL Server 是一种端口型数据库，任何人都可以通过分析工具连接到数据库上，从而绕过操作系统的安全机制，进而闯入系统，破坏、窃取数据资料。SQL Server 2000 作为通过美国政府 C2 级安全认证的系统，已经具备较高的安全机制。通过恰当的安全配置，可以更好发挥 SQL Server 的安全性。

3. 实验环境

运行 Windows 2000 Server 主机一台，安装 SQL Server 2000 软件。

4. 实验内容

(1) 安装 SQL Server 2000 最新的补丁程序,进行安全性升级;
(2) 基于 SQL Server 2000 内部安全机制进行相关设置。

5. 实验步骤

(1) 获取 SQL Server 2000 最新补丁程序 SQL Server 2000 Service Pack4(SP4)进行升级,如图 4.99 所示。



图 4.99 升级 SQL Server 程序

(2) 在 SQL Server 企业管理器中选择一个服务器,单击右键选择"属性",在弹出的对话框中选择"安全性"选项卡,设置 SQL Server 2000 身份验证为"仅 Windows"系统认证模式,如图 4.100 所示。

(3) 在企业管理器中展开一个服务器,选择"安全性"中的"登录"图标,双击 sa,在弹出的对话框中为 sa 设置一个强壮的口令,如图 4.101～图 4.103 所示。

(4) 展开一个服务器组,打开其属性对话框,选中审核级别中的"失败"单选按钮,对 SQL Server 的连接进行审核,如图 4.104 所示。

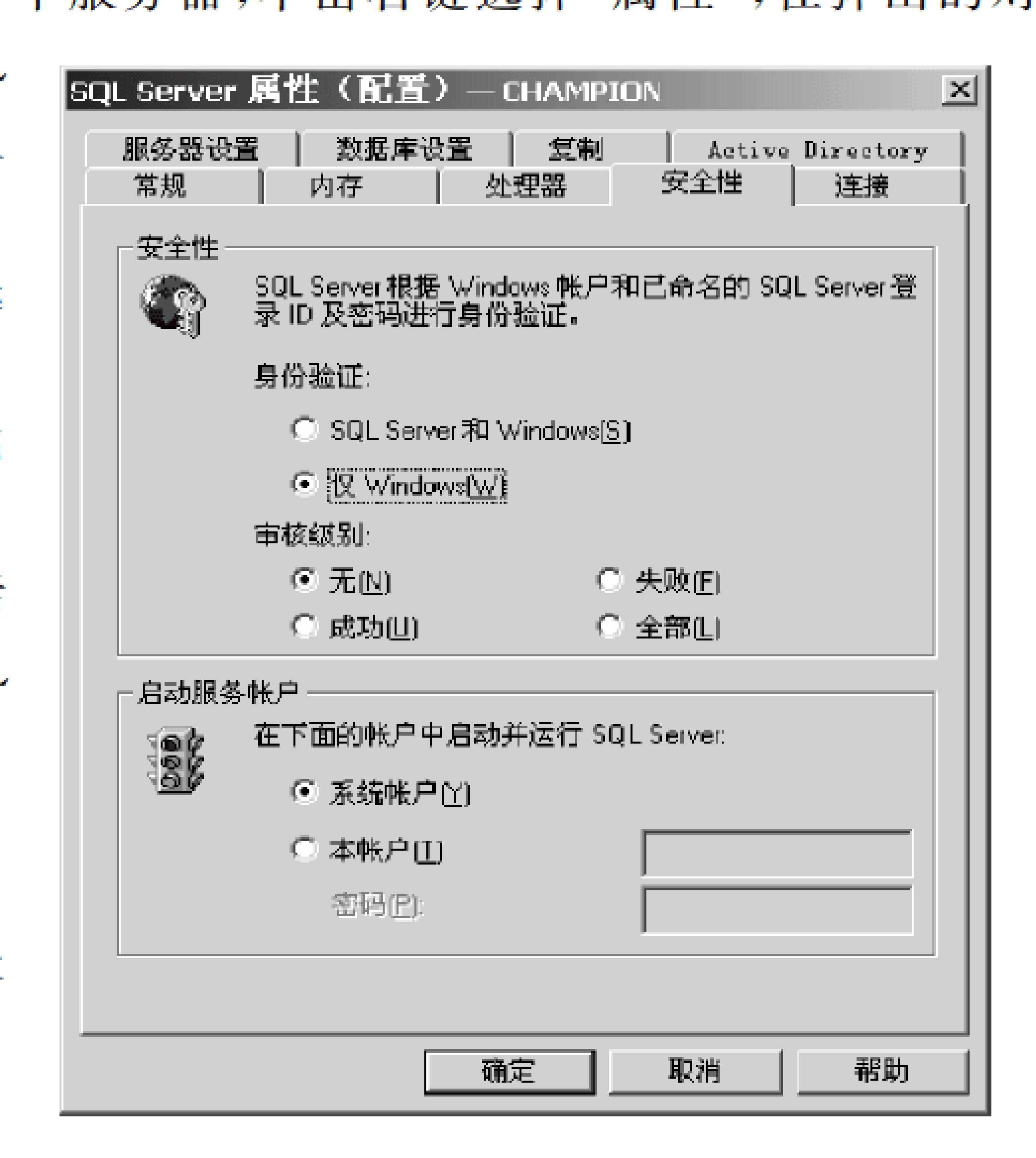


图 4.100 设置身份认证方式

6. 实验报告与要求

根据上面介绍的各项实验要求,详细观察记录 SQL Server 2000 安全设置前后的变化,给出分析报告。

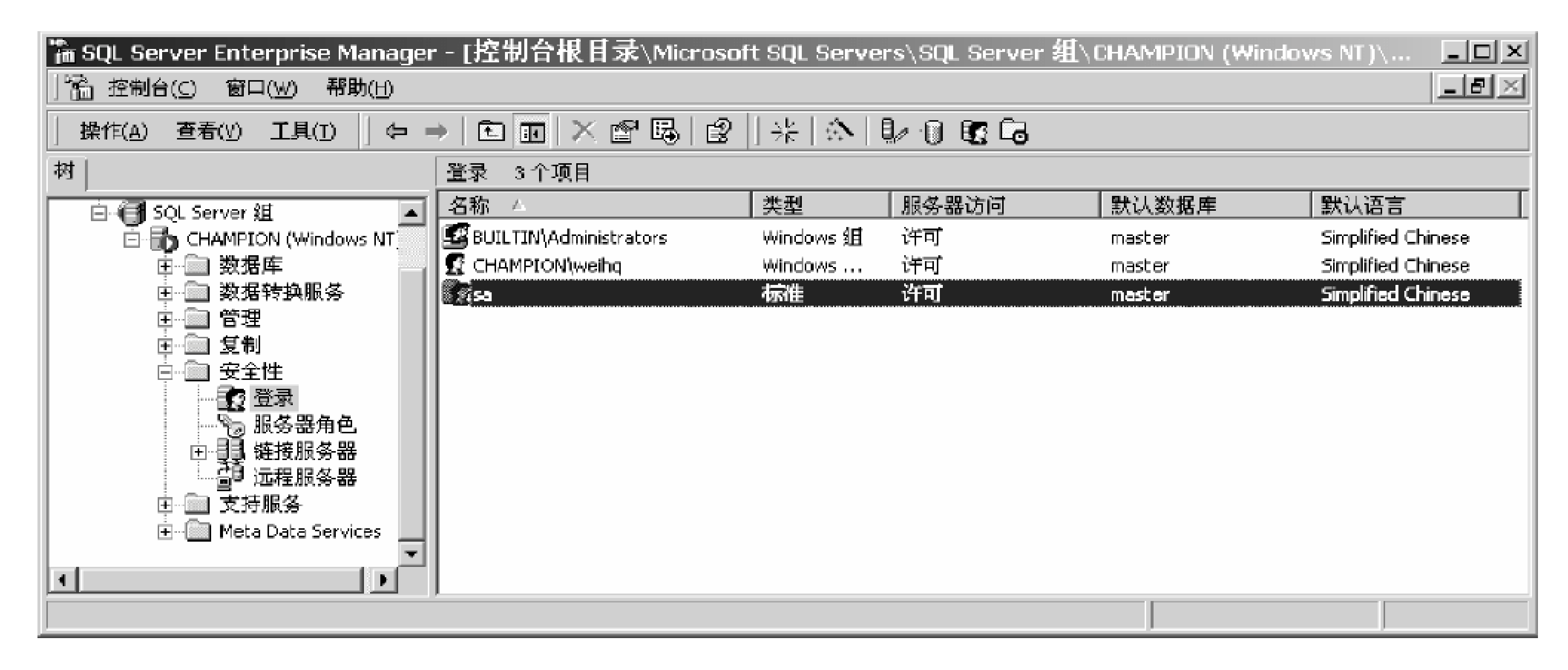


图 4.101 为 sa 设置口令



图 4.102 设置 sa 口令(1)



图 4.103 设置 sa 口令(2)

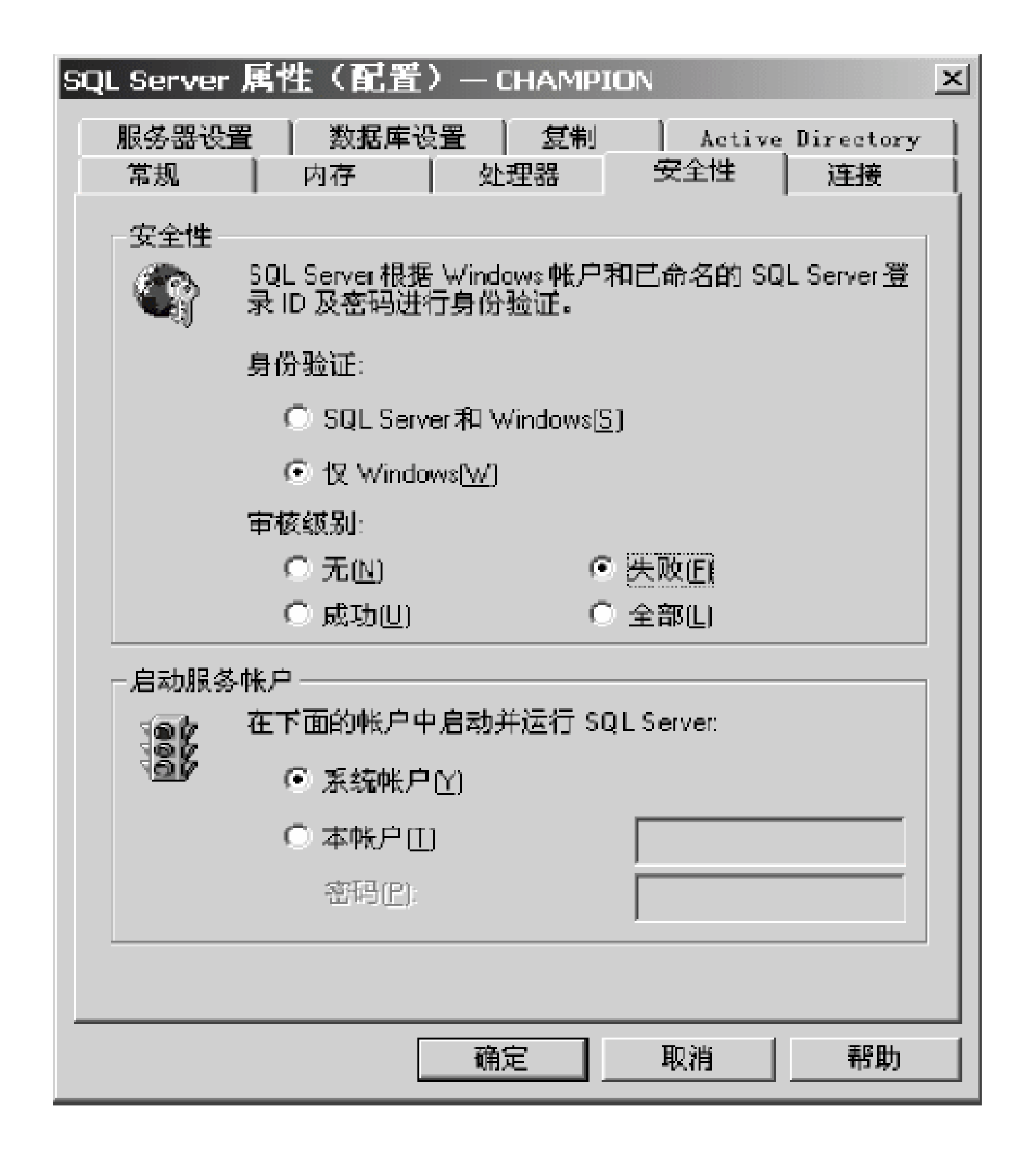


图 4.104　设置审核方式

7. 实验分析与讨论

为了提高数据库的网络安全性，可以配置系统防火墙过滤针对 SQL Server 相应端口的外来数据包。用户可以自行确定 SQL Server 2000 相应端口并进行设置。另外，微软的安全基准分析器 MBSA 可以对 SQL Server 2000 中的不安全设置进行扫描，用户可以尝试用该工具对已配置的 SQL Server 2000 的安全性进行评估。

8. 注意事项

（1）SQL Server 2000 中大多数安全设置都需要系统重启后才能生效。

（2）数据库系统管理员需要经常查看数据库事件日志记录，及时发现问题进行解决，日志文件最好存放到一个不同于数据文件存放的硬盘中。

第5章

信息系统综合安全管理

5.1 实验基础

对安全技术和产品的选择运用，只是信息安全实践活动中的一部分。信息安全更广泛的内容，还包括制定完备的安全策略，通过风险评估来确定需求，根据需求选择安全技术和策略，并按照既定的安全策略和流程规范来实施、维护和审查安全控制措施。管理在信息保障中的作用越来越得到重视，计算机信息安全对策包含三个方面：安全立法、行政管理和安全技术，其中前两项属于管理的范畴。

5.1.1 计算机信息安全立法与行政管理

关于计算机犯罪，各国的法律都有自己的定义。在中国的相关法律中提出，所谓计算机犯罪指与计算机相关的危害社会并应加以处罚的行为。计算机犯罪具体表现有：装入欺骗性数据、未经批准使用资源、窜改窃取信息、盗窃与诈骗电子财物和破坏计算机资产等。

计算机犯罪具有收益高、时效快、风险低、无痕迹、无国界地界、危害大等特点，20世纪80年代以来成为各国日益严重的社会问题。各国针对该问题都进行了系列相关法律法规的建设工作。我国已有的计算机信息安全法律法规有：《中华人民共和国计算机信息系统安全保护条例》、《中华人民共和国保守国家秘密法》、《计算机软件保护条例》、《中华人民共和国计算机网络国际互联网管理暂行规定及实施办法》、《中国公众媒体通信管理办法》、《计算机病毒控制条例》、《中华人民共和国计算机信息系统安全检查办法》和《中华人民共和国计算机信息系统安全申报注册管理办法》等。

计算机安全行政管理包括人员的教育与培训和健全机构岗位设置及规章制度。通常的信息安全规章制度有：

(1) 岗位责任制：制定各类人员的岗位责任制，特别强调严格纪律、严格管理、严格分工的原则，不准串岗，严禁程序设计师同时担任系统操作员，严格禁止系统管理员、终端操作员和系统设计员混岗。专职安全管理人员负责本系统区域内安全策略的实现，保证安全策略的长期有效，负责软硬件的安装维护、日常操作监视、应急条件下安全措施的恢复和风险分析等。安全审计人员监视系统运行情况，收集对系统资源的各种非法访问事件，并对非法

事件进行记录、分析和处理，必要时将审计事件上报主管部门。保安人员负责非技术性常规安全工作。

（2）运行管理维护制度：包括设备管理维护制度、软件维护制度、用户管理制度、密钥管理制度、出入门卫管理值班制度、各种操作规程、各种行政领导部门的定期检查及监督制度等。

（3）计算机处理控制管理制度：包括数据处理流程的编制和控制、程序软件和数据的管理、拷贝移植和存储介质的管理、文件档案日志的标准化、通讯网络系统的管理。

（4）文档资料管理制度：非计算机的各种凭证、单据、帐簿、报表和文字资料，要妥善保管和严格控制。记帐必须交叉复核。各类人员所掌握的资料要与其身份匹配，如终端操作员只能阅读终端操作规程、手册，只有系统管理员才能使用系统手册。

5.1.2 信息系统安全标准

信息系统的安全标准可以规范系统的建设和使用，规范人们的安全防范行为，使人们的信息安全意识提高到必要的水平。因此，信息系统的安全标准是实现安全信息系统极为重要的环节。发达国家在系统安全标准方面的研究工作起步相对较早。

美国国防部在 1983 年制定了可信计算机系统评价准则（TCSEC），它将计算机系统的安全功能和可信任度综合在一起考虑，为计算机安全产品的评测提供了测试方法。TCSEC 进行系统安全等级评估的依据有以下几种。

（1）安全策略：必须有一个明确的、确定的由系统实施的安全策略；

（2）识别：必须唯一而可靠地识别每个主题，以便检查主体/客体的访问请求；

（3）标记：给每个客体一个标号，并指明该客体的安全级别；

（4）可检查性：系统对影响安全的活动必须维持完全而且安全的记录；

（5）保障措施：系统含实施安全性的机制并能评价其有效性；

（6）连续的保护：实现安全性的机制必须受到保护以防止未经批准的改变。

TCSEC 将安全分为如下 7 个级别。

（1）D 级：最小保护。没有访问限制，DOS、Windows 3.x/95 等系统采用该安全级别。

（2）C1 级：自主存取控制。具有一定的硬件安全级，用户需要认证，但不能控制用户级别，如早期的 UNIX。

（3）C2 级：可控访问保护。进一步访问权限控制，身份验证级别，广泛的审核跟踪，如 UNIX、Windows NT。

（4）B1 级：标记安全保护。对每个对象都实施保护，支持多级安全，强制存取控制，适用于政府机构和防御系统。

（5）B2 级：结构化保护。所有对象均加标签，给设备分配安全级别，使较高安全级别可与较低安全级别系统通信，取消特权用户。

（6）B3 级：安全域。要求用户通过一条可信任途径连接到系统上，硬件保护系统的数据存储区，区分系统管理员、系统操作员和系统安全员的职责。具有高抗渗透能力，即使系统崩溃也不会泄密。

（7）A1 级：验证设计。附加一个安全系统的受监视设计，所有系统部件来源有安全保证，规定安全系统运送、安装的程序。

1989 年，国际标准化组织 ISO 在信息系统安全体系结构标准 ISO 7498-2 中描述了开放互连 OSI 安全体系结构的 5 种安全服务项目：

- 鉴别；
- 访问控制；
- 数据保密；
- 数据完整；
- 抗否认。

为了实现以上功能，ISO 7498-2 提出了 8 种标准安全机制：

- 加密机制；
- 数字签名机制；
- 访问控制机制；
- 数据完整性机制；
- 鉴别交换机制；
- 通信业务填充机制；
- 路由控制机制；
- 公证机制。

其他的安全标准还有英、法、荷、德四国于 20 世纪 90 年代提出的欧洲信息技术安全评价准则 ITSEC、加拿大 1993 制定的 CTCPEC 评价标准和美国 1993 年提出的联邦准则 FC 等。我国于 1994 年，由国务院发布了《中华人民共和国计算机信息系统安全保护条例》，规定计算机实行安全等级保护。1995 年，又分别出台了《信息处理系统开放互联基本参考模型第 2 部分安全体系结构》、《信息处理数据加密实体鉴别机制第Ⅰ部分：一般模型》、《信息技术设备的安全》等。1999 年公安部制定了《计算机信息系统安全保护等级划分准则》，并于 2001 年 1 月 1 日起实施，该准则中提出 5 个计算机安全保护级别：

- 用户自主保护级；
- 系统审计保护级；
- 安全标记保护级；
- 结构化保护级；
- 访问验证保护级。

5.1.3 信息系统安全审计

信息系统安全审计是以信息系统安全体系、策略、人和流程等为对象的深入细致的检查，目的是为了找出信息系统安全体系中薄弱环节并给出相应的解决方案。

安全审计的基本内容分为两步。首先，检查实际工作是不是按照现有规章制度进行。其次，对审计步骤进行调整和编排，更好地判断出安全事件的发生地点或来源。审计工作本身也需要保护。需要进行审计的事件主要包括：系统登录活动、文件读写活动、改变系统或网络优先级的活动。需要进行审计的对象包括敏感数据、数据的保密区域以及各种资源等。有些对象需要专门的审计，而且有些数据可能非常重要，针对它们的每一次访问都必须记录下来，包括事件的类型或者名称、事件发生的日期和时间、事件成功与否、有关的程序名称或

文件名等。企图绕过系统保护机制和系统审计监控功能的攻击尝试随时都会发生，为了更有效地检测、发现和挫败来自内外两方面的这类企图，审计过程应该对与安全有关的事件进行合理的编排。审计流程需要做到以下几点：

（1）对系统用户来说是透明的；

（2）支持各种审计软件；

（3）在调整和编排有关审计事件时应是完备的和精确的；

（4）应保证与审计工作有关的文件的安全性。

安全审计工作主要分两大类：一种是单位自行完成的内部审计，另一种是由外部专业公司或人员完成的外部审计。内部审计的主要目的是检查内部各部门对安全制度的遵守情况，可以由一个比较正规的内部审计组织来完成，也可以不那么正规。由第三方完成的审计都非常正规和深入。

由审计方负责的工作包括制定和实施审计或评估工作的流程、选择需要审计的事件、对审计记录进行复查、维护和保护审计数据、定期复查审计参数等。需要进行审计的事件主要包括敏感数据、数据的保密区域以及各种资源等等。信息系统安全审计工作首先需要制定出审计计划，其次需要选择相关的审计工具，如相关技术文档、安全审计软件、测试程序等，此外，还需要根据审计结论给出相应的改进措施。

对于被审计方来说，首先需要全力配合安全审计人员对网络的安全措施进行测试。审计工作中所发现的一些严重的问题可能不在自己的控制范围内而出在外包的工作部分，因此最好在审计工作开始之前提前通知供应商，让他们参加到与他们提供的服务有关的分析讨论中来。在与安全审计机构签约时，需要考虑以下因素：

（1）一定要在合同里加上保密条款，约束对方不得泄露有关信息。另外，合同里必须写明进行本次评估的公司对它提交的报告不得保有任何权利；

（2）要求安全审计机构先提供它准备派遣的审计师的个人简历，以对他们的技术和经验有一个了解，挑选优秀的审计师来进行审计；

（3）在合同里加上知识转移条款，保证本单位员工能够研究和学习审计师所使用的方法和流程。

一份完整的安全审计大纲应该包括：安全措施的管理、安全策略和制度、相关的标准和流程、技术性安全措施、对安全措施的评估、文档、事故响应、对安全措施进行测试、物理防护措施、个人因素、法律方面的考虑、安全意识、培训和教育、企业组织结构方面的因素等。

5.1.4 信息系统安全体系的设计

计算机安全问题是伴随着计算机的发展而产生的，随着计算机应用模式由主机终端方式发展到目前的互联网阶段，安全问题变得越来越复杂和重要。计算机系统中的安全威胁来源于各种自然灾害等不可抗拒因素、外部的各种恶意攻击、系统本身的安全缺陷、各种应用软件漏洞等。因此，广义计算机信息安全包括信息设备的物理安全性、场地环境保护、物理硬件安全、病毒、通讯设备的信息安全、网络安全等。

计算机信息系统的安全需求有以下几方面。

（1）保密性：信息不被泄露给非授权的用户、实体或过程，包括物理保密和信息加密；

(2) 真实性：身份的可鉴别性，不可假冒；

(3) 完整性：信息未经授权不能进行改变的特性，面向信息；

(4) 可靠性：系统能够在规定条件和规定的时间内完成规定的功能的特性，包括稳定性、抗毁性、生存性和有效性等方面；

(5) 服务可用性：信息和服务可被授权实体访问并按需求使用的特性，该特性是面向用户的；

(6) 不可否认性：信息交互过程中，确认参与者的真实同一性；

(7) 可控性：对(网络)信息的传播及内容具有控制能力的特性。

为了满足以上安全需求，通常采用的计算机信息安全对策包括三个方面：安全立法、行政管理、技术措施。在制定安全对策时，通常需要遵守以下原则：

- 综合平衡代价原则
- 整体综合分析与分级授权原则
- 方便用户原则
- 灵活适应性原则
- 可评估性原则

计算机信息安全具有以下四大特性：

(1) 计算机安全是一个系统概念，不仅仅是技术问题，更重要的是管理问题，还与社会道德、行业管理及人们的行为模式紧密联系。

(2) 计算机安全是相对的，不存在永远攻不破的安全系统。

(3) 计算机安全是有代价的，进行计算机安全方案的制订是安全、成本和速度的权衡。

(4) 计算机安全是发展的、动态的，网络的攻与防此消彼长，安全技术具有强竞争性和对抗性，必须不断评估调整，安全是一个过程而非终点。

因此，信息安全的建设是一个系统工程，它需要对信息系统的各个环节进行统一的综合考虑、规划和构架，并时时兼顾组织内外不断发生的变化，任何环节上的安全缺陷都会对系统构成威胁。正确的做法是遵循国内外相关信息安全标准与最佳实践过程，考虑对信息安全的各个层面独特需求，在风险分析的基础上引入恰当控制，建立合理的安全管理体系；另一方面，这个安全体系还应当随着环境的变化、业务的发展和信息技术的提高而不断改进，不能一劳永逸，一成不变。信息安全的实现是一个需要完整的技术和管理体系来保证的连续过程。

5.2 实验项目

5.2.1 信息系统安全审计

1. 实验目的

了解信息系统安全审计的主要作用和基本流程，掌握制订安全审计计划的方法。

2. 实验原理

进行安全审计工作之前首先需要设计一个审计计划，不同的系统有不同的应用环境和

内部结构，因此，具体的审计过程和内容也是不一样的。制订审计计划时，需要详细分析系统构成和应用单位需求，通常审计计划中应包括安全策略、制度、相关标准和流程、安全技术措施、文档管理、事故响应、个人因素、法律因素、安全意识、培训和教育等方面。审计方可以根据计划来搜集充分的相关数据，并选择恰当的审计工具，为审计工作的开展做好前期准备。

3. 实验环境

目标信息系统的调研环境。

4. 实验内容

（1）调研获取某目标信息系统的基本情况，分析其安全需求；
（2）针对目标信息系统制订出安全审计计划；
（3）针对可能审计出的安全问题，给出相应的解决措施。

5. 实验步骤

（1）通过资料查阅和调研获得目标审计信息系统的基本结构和应用背景，确定该系统的安全需求；

（2）制订安全制度和标准的审计计划，具体内容包括：信息安全策略和规章制度、信息的分类和价值评估、数据的保密性、数据的完整性、数据的重要性、数据的可审计性、系统管理机构的特权管理、信息的访问控制措施、安全事件的上报程序、突发事件响应计划、员工信息不泄露条款等；

（3）制订物理安全审计计划，包括机房管理、网络设施管理、文档管理等；

（4）制订网络安全审计计划，包括密钥管理、日志管理、网络用户管理、防火墙管理、其他网络安全工具管理等；

（5）制订应用软件安全审计计划，包括软件资源管理、软件权限管理等；

（6）制订备份审计和突发事件审计计划；

（7）分析可能出现的重要安全问题；

（8）针对可能出现的问题给出相应解决方案。

6. 实验报告与要求

根据上面介绍的各项实验要求，制订目标系统的审计计划，针对可能发现的问题，给出相应的解决措施，撰写实验分析报告。

7. 实验分析与讨论

在实现以上制订出的审计计划时，需要用到哪些辅助审计工具，尝试了解这些审计工具的使用方法。

8. 注意事项

（1）内部审计可以由一个比较正规的内部审计组织来完成，也可以不那么正规。审计工作的伸缩性很大，简单的可以只检查一下系统日志，复杂的则可以对人员、策略、制度流程

等所有方面进行细致的审查,用户可以根据需要进行选择;

(2)本实验提供的安全审计步骤仅包含主要方面,用户可以根据系统具体需求增减部分内容来完成审计计划的制订。

5.2.2 日常操作安全规程制订

1. 实验目的

了解安全管理制度的重要性,掌握日常操作安全规程的制订方法。

2. 实验原理

信息系统日常操作安全规程是安全管理制度的一部分,对信息系统的日常使用人员、权限、方法等进行详细规定,并明确职责。使信息系统的安全策略和制度可以得到真实的贯彻执行,是信息系统安全的重要保障。制定日常操作安全规程时,主要基于多人负责、任期有限、职责分离等原则。

3. 实验环境

目标信息系统的调研环境。

4. 实验内容

(1)制订计算机上机管理制度;
(2)制订用户帐户管理制度;
(3)制订信息保护管理制度;
(4)制订远程访问管理制度;
(5)制订特殊访问权限管理制度。

5. 实验步骤

(1)以小组为单位确定目标信息系统,并对系统基本情况和操作人员构成进行调研;
(2)确定信息系统的安全需求;
(3)确定系统相关人员的构成类型;
(4)确定主要系统资源和主要日常业务流程和操作;
(5)明确各类人员对资源的操作权限、方法;
(6)结合业务和相关人员制订具体的操作规程;
(7)制订相应的规程执行情况审计方法,并明确各人员职责;
(8)制订操作规程的管理方法和管理人员职责;
(9)制订用户帐户的管理方法。

6. 实验报告与要求

根据上面介绍的各项实验要求,制订目标系统的日常操作安全规程,撰写实验报告。

7. 实验分析与讨论

日常操作安全规程如何与系统的安全需求和安全策略相一致，制订操作规程时，如何体现多人负责、任期有限、职责分离等原则。

8. 注意事项

（1）信息系统的相关人员通常包括员工、普通管理人员、系统管理员、系统安全管理员、内部审计人员、应用软件开发人员、计算机操作员、网络管理员、技术支持人员以及其他人员等，不同系统会有不同的岗位设置；

（2）操作安全规程可以把通常以制度、流程或合同方式规定的人员安全责任进一步明确和具体化。

5.2.3　应急响应方案制订

1. 实验目的

了解预先制订应急响应方案的必要性，掌握针对目标系统进行分析和制订应急响应方案的方法。

2. 实验原理

应急响应通常指人们为了应对各种紧急事件的发生所做的准备以及在事件发生后所采取的措施。无论信息系统的运行环境多么安全，被攻击的风险依然存在。在遭受攻击后才对安全事件作出反应要比及时作出反应的代价高出很多，因此系统的安全策略中必须包含有关单位如何响应不同类型攻击和紧急情况的详细说明。虽然对事件的响应中多数操作由应急小组执行，但各级 IT 人员应该知道如何在内部报告安全事件。应急响应方案可以使信息环境中的所有成员知道在发生事件时应做什么。

3. 实验环境

目标系统的调研环境。

4. 实验内容

（1）确定应急响应角色的责任；
（2）制订紧急事件提交策略；
（3）规定应急响应优先级；
（4）安全事件的调查与评估方法；
（5）制订应急响应相关补救措施；
（6）确定应急紧急通知机制。

5. 实验步骤

（1）调研目标系统基本情况；
（2）对系统可能遭受的安全风险进行分类并确定响应优先级；

（3）确定安全事件中可能涉及的人员；
（4）制订安全事件的检测和通报机制；
（5）制订安全事件的初步评估方法，确定破坏的类型和严重程度；
（6）制订对危害抑制的策略和措施，控制损失，将风险降低到最小；
（7）制订彻底清除危害源的流程；
（8）制订系统恢复计划；
（9）制订对外部机构的事件通知流程；
（10）制订事件记录方法及总结整理事件记录的流程。

6. 实验报告与要求

根据上面介绍的各项实验要求，制订目标系统的应急响应计划，给出实验报告。

7. 实验分析与讨论

了解事件响应关键技术除入侵检测技术和系统备份与灾难恢复技术外，还有哪些，分别可以应用于什么阶段。国内外目前已经建立了众多的应急响应组织，对他们的基本作用和发展情况进行了解。

8. 注意事项

（1）应急响应中的角色主要包括用户、安全管理员、安全审计员、信息发布部门、管理层等；
（2）制订应急响应计划时，应注意保护事件的相关证据。

5.2.4 个人用户计算机系统安全方案设计

1. 实验目的

了解个人计算机系统存在的安全风险，制订相应的安全策略，并部署完整的安全解决方案。

2. 实验原理

个人计算机系统主要是为了满足用户在工作、学习和生活上的需要，其安全需求和安全策略的制订都和企业级系统有较大的不同。了解并掌握个人计算机的安全保障方法对于综合运用计算机信息安全知识和实现组织信息安全都有很好的帮助。

3. 实验环境

不同配置的个人用户计算机一台。

4. 实验内容

（1）分析个人电脑可能面临的安全风险；

（2）制订个人计算机系统安全策略；
（3）制订全面完整的个人计算机系统安全解决方案并进行部署。

5. 实验步骤

（1）分析个人计算机系统的主要功能需求和基本结构；
（2）分析个人计算机面临的安全风险类型；
（3）制订个人计算机基本安全策略；
（4）制订计算机病毒软件等常用防护工具的部署、使用和维护计划；
（5）制订关键资源和数据的保护方法；
（6）制订个人数据的备份计划；
（7）制订帐户日常管理方法；
（8）制订个人计算机的日常操作安全规程；
（9）进行概要的安全方案成本核算，分析方案的经济可行性；
（10）根据以上方案对目标计算机进行安全部署。

6. 实验报告与要求

针对个人计算机用户使用需求制订一份安全解决方案，并在个人计算机上实施，比较并分析方案实施前后系统的不同，撰写相应的实验报告。

7. 实验分析与讨论

请用户思考个人计算机的安全方案与企业级信息系统的安全方案的不同体现哪些地方。针对已部署好的安全方案，选择常见的探测和攻击工具检测系统的安全性。

8. 注意事项

用户可以针对自己日常使用的 PC 进行本实验的安全方案制订。

5.2.5 电子政务网站整体信息安全解决方案设计

1. 实验目的

了解电子政务网站系统的结构，分析电子政务网站的安全需求，制订适当的安全策略，针对特定应用背景提出一套整体的安全解决方案。

2. 实验原理

电子政务是政府在其管理和服务职能中运用现代信息和通信技术来实现政府组织结构和工作流程的重组优化的一种新型机制，可以超越时间、空间和部分分隔的制约，全方位地向社会提供优质、规范、透明的服务，是政府管理理念和管理手段的变革。电子政务系统主要包括两大部分：内部政务办公系统和对外服务部分，后者即电子政务网站系统。

电子政务网站系统的安全风险有：非法用户通过公共网络进入内部网内各级局域网系

统，以获取资源或支配资源；篡改向社会公布的政务信息以制造混乱；插入和修改传输中的数据；窃听和截获传输数据；假冒管理者和信息主体发布虚假信息。因此，在电子政务系统与Internet连接部分，存在的安全需求有：完整性保护、源鉴别服务、用户鉴别和访问控制等。

3. 实验环境

目标电子政务系统的调研环境。

4. 实验内容

（1）确定目标行政管理机构所采用的信息系统的安全需求；
（2）确定目标电子政务网站的安全策略；
（3）进行安全解决方案设计。

5. 实验步骤

（1）了解目标行政管理机构的基本情况和信息系统结构；
（2）确定目标电子政务网站的安全需求；
（3）制订网站系统的基本安全策略；
（4）分析网站系统的信任链结构，确定信任服务体系结构；
（5）基于业务分析确定所需采用的信任保障技术；
（6）确定基于身份认证的用户权限管理机制；
（7）网络安全工具的配置方案；
（8）网络硬件设施管理方法；
（9）确定数据库安全保障机制。

6. 实验报告与要求

针对目标电子政务网站制订一份安全解决方案，撰写相应的实验报告。

7. 实验分析与讨论

请用户思考电子政务信息系统与其他系统相比较在软硬件平台和安全技术采用方面有哪些特殊需求。

8. 注意事项

（1）为便于用户对整个系统的把握，建议选择小型行政管理机构进行安全方案设计；
（2）信任体系是电子政务系统安全机制的核心部分，实验中应重点对CA体系的设计进行思考。

5.2.6 电子商务网站整体信息安全解决方案设计

1. 实验目的

了解电子商务网站系统的结构，分析电子商务网站的安全需求，制订适当的安全策略，

针对特定应用提出一套整体的网络安全解决方案。

2. 实验原理

电子商务网站系统提供了一个参与商业活动的个人、公司、商业集团等之间的交易和结算平台。在电子商务活动中存在的安全风险有：非法用户通过网络进入系统；窃取或修改数据进行电子犯罪；与系统人员勾结、联合进行诈骗；假冒他人行骗；窃用信用卡或购物卡；篡改商务信息、制造混乱；抵赖已发生的交易或交易的内容。针对以上风险，电子商务网站有完整性保护、源鉴别服务、数字签名、抗抵赖服务、身份鉴别、访问控制和加密等安全需求。

3. 实验环境

目标电子商务网站的调研环境。

4. 实验内容

（1）确定目标电子商务企业所采用的网站系统的安全需求；
（2）确定目标电子商务网站的安全策略；
（3）进行安全解决方案设计。

5. 实验步骤

（1）了解目标电子商务企业的基本业务情况、运营方式和网站结构；
（2）评估网站系统的资产和安全风险，确定目标电子商务网站系统的安全需求；
（3）制订网站系统的基本安全策略；
（4）选择系统采用的安全交易协议，并确定基于该协议的业务实现过程；
（5）制订基于 PKI 的交易各方身份认证方法，确定信任服务体系结构；
（6）基于业务分析确定所需采用的信任保障技术；
（7）确定用户权限管理机制；
（8）网络服务器安全工具的配置方案；
（9）网络通信硬件设施管理方法；
（10）确定商业数据安全性保障机制。

6. 实验报告与要求

针对目标电子商务网站制订一份安全解决方案，撰写相应的实验报告。

7. 实验分析与讨论

了解国内外各大电子商务网站采用的具体安全解决方案，并进行比较分析。

8. 注意事项

（1）用户可以利用硬件和软件的冗余技术来保障电子商务网站的服务可用性和数据安全性；

（2）对于电子商务系统，密钥的管理非常重要。构建基于PKI的信息体系时，可以选择可信的政府部门和法律执行部门作为合法的第三方密钥托管机构。

5.2.7 企业内部信息系统信息安全方案设计

1. 实验目的

了解目标企业目前所采用的信息系统安全方案，掌握部署安全方案的方法，根据网络环境的不同以及用户提出的不同需求，提出一套整体安全解决方案。

2. 实验原理

随着国内计算机和网络技术的迅猛发展和广泛应用，各企业都已构建了满足自身业务需要的信息系统，重要的业务数据大都以电子形式存储于系统数据库中，企业的运营越来越依赖于信息系统的支持。企业信息系统通常包含内部系统和外部网络系统两部分。两者之间可以通过一定的网络安全技术进行隔离。对于企业来讲，重要的信息资源往往集中于内部信息系统中，因此针对内部网络进行安全方案设计和部署尤为重要。

3. 实验环境

目标企业的背景信息调研环境。

4. 实验内容

（1）确定目标企业内部信息系统的安全需求；
（2）确定目标企业的安全策略；
（3）基于目标企业现有安全措施进行安全解决方案设计。

5. 实验步骤

（1）了解目标企业的基本业务情况和内部信息系统结构；
（2）确定信息系统的安全需求；
（3）制订系统的基本安全策略；
（4）制订相关安全制度和规程；
（5）确定用户权限管理机制；
（6）制订计算机病毒软件等常用防护工具的部署、使用和维护计划；
（7）制订关键资源和数据的保护方法；
（8）制订重要数据的备份计划；
（9）制订应急响应计划；
（10）制订硬件设施管理维护机制。

6. 实验报告与要求

针对目标企业制订一份完整安全解决方案，撰写相应的实验报告。

7. 实验分析与讨论

了解部分企业的现有安全方案，比较分析他们的优缺点。

8. 注意事项

（1）对企业内部信息系统安全方案设计时，可以对网络安全部分进行简化，重要考虑企业内部人员和资源的管理；

（2）用户也可以选择某虚拟企业为对象进行安全方案设计，设计之前首先需要明确企业的业务内容。

参 考 文 献

［1］ 陈兵，等. 网络安全与电子商务. 北京：北京大学出版社，2002

［2］ 张世永. 网络安全原理与应用. 北京：科学出版社，2003

［3］ 钱钢. 信息系统安全管理. 南京：东南大学出版社，2004

［4］ 王常吉，龙冬阳. 信息与网络安全实验教程. 北京：清华大学出版社，2007

［5］ 鲁珂，等. 计算机信息系统安全实验教程. 北京：电子科技大学出版社，2007

［6］ 高敏芬，贾春福. 信息安全实验教程. 天津：南开大学出版社，2007

读者意见反馈

亲爱的读者：

感谢您一直以来对清华版计算机教材的支持和爱护。为了今后为您提供更优秀的教材，请您抽出宝贵的时间来填写下面的意见反馈表，以便我们更好地对本教材做进一步改进。同时如果您在使用本教材的过程中遇到了什么问题，或者有什么好的建议，也请您来信告诉我们。

地址：北京市海淀区双清路学研大厦 A 座 602 室　计算机与信息分社营销室　收

邮编：100084　　　　电子邮箱：jsjjc@tup.tsinghua.edu.cn

电话：010-62770175-4608/4409　　　　邮购电话：010-62786544

教材名称：计算机信息安全管理实验教程

ISBN：978-7-302-22201-9

个人资料

姓名：＿＿＿＿＿＿　年龄：＿＿＿＿所在院校/专业：＿＿＿＿＿＿＿＿＿＿

文化程度：＿＿＿＿　通信地址：＿＿＿＿＿＿＿＿＿＿＿＿＿＿＿＿＿＿＿＿

联系电话：＿＿＿＿　电子信箱：＿＿＿＿＿＿＿＿＿＿＿＿＿＿＿＿＿＿＿＿

您使用本书是作为：□指定教材 □选用教材 □辅导教材 □自学教材

您对本书封面设计的满意度：

□很满意 □满意 □一般 □不满意　改进建议＿＿＿＿＿＿＿＿＿＿＿＿＿＿

您对本书印刷质量的满意度：

□很满意 □满意 □一般 □不满意　改进建议＿＿＿＿＿＿＿＿＿＿＿＿＿＿

您对本书的总体满意度：

从语言质量角度看　□很满意 □满意 □一般 □不满意

从科技含量角度看　□很满意 □满意 □一般 □不满意

本书最令您满意的是：

□指导明确 □内容充实 □讲解详尽 □实例丰富

您认为本书在哪些地方应进行修改？(可附页)

＿＿＿＿＿＿＿＿＿＿＿＿＿＿＿＿＿＿＿＿＿＿＿＿＿＿＿＿＿＿＿＿＿＿＿＿

＿＿＿＿＿＿＿＿＿＿＿＿＿＿＿＿＿＿＿＿＿＿＿＿＿＿＿＿＿＿＿＿＿＿＿＿

您希望本书在哪些方面进行改进？(可附页)

＿＿＿＿＿＿＿＿＿＿＿＿＿＿＿＿＿＿＿＿＿＿＿＿＿＿＿＿＿＿＿＿＿＿＿＿

＿＿＿＿＿＿＿＿＿＿＿＿＿＿＿＿＿＿＿＿＿＿＿＿＿＿＿＿＿＿＿＿＿＿＿＿

电子教案支持

敬爱的教师：

为了配合本课程的教学需要，本教材配有配套的电子教案(素材)，有需求的教师可以与我们联系，我们将向使用本教材进行教学的教师免费赠送电子教案(素材)，希望有助于教学活动的开展。相关信息请拨打电话 010-62776969 或发送电子邮件至 jsjjc@tup.tsinghua.edu.cn 咨询，也可以到清华大学出版社主页(http://www.tup.com.cn 或 http://www.tup.tsinghua.edu.cn)上查询。

高等学校教材・信息管理与信息系统
系列书目

ISBN	书　名	作　者	定　价
9787302127079	IT 项目建设与管理精选案例分析	杨坚争等	24.00
9787302144649	Oracle 数据库管理及应用开发教程	吴京慧等	39.00
9787302136095	SQL Server 数据库管理与开发	肖慎勇等	36.00
9787302136101	电子商务安全技术	张爱菊	24.00
9787302136750	电子商务概论	朱少林等	29.00
9787302188391	电子商务技术基础(第 2 版)实验指导与习题解答	张宝明等	26.00
9787302172390	电子商务技术基础(第 2 版)	张宝明等	29.80
9787302136255	电子商务实现技术	吴泽俊	36.00
9787302136088	电子商务系统规划与设计	骆正华	32.00
9787302136248	多媒体技术与应用	阮新新	29.00
9787302164319	管理信息系统及其开发	程学先	39.00
9787302164821	国际贸易电子商务	刘咏芳	29.00
9787302128069	会计信息系统实务教程	陈福军等	49.00
9787302153177	会计信息系统实务教程学习指南与实验指导	陈福军等	24.00
9787302109778	经济信息管理	刘腾红	29.00
9787302180562	企业信息化	赵守香等	39.00
9787302135067	审计知识工程	陈耿等	23.00
9787302179726	数据库系统应用教程	王成等	23.00
9787302179702	数据库系统应用实验教程	王成等	18.00
9787302106371	网络信息系统的分析设计与评价 ——理论・方法・案例	赵玮等	42.00
9787302108184	现代 IT 服务管理 ——基于 ITIL 的最佳实践	曹汉平等	25.00
9787302164661	现代信息检索实用教程	郑成增	29.00
9787302118930	信息管理导论	宋克振等	39.00
9787302144366	信息检索与分析利用	谢德体等	18.50
9787302149514	信息系统开发工具 ——PowerBuilder 语言	张瑞军等	29.00
9787302124290	信息系统开发与 IT 项目管理	曹汉平	34.00
9787302115830	信息资源管理	张凯等	29.00
9787302159414	信息资源管理(第二版)	张凯等	35.00
9787302182580	网络数据库原理与应用	刘翔	21.00